The vCISO

Supplemental – Information Security Policy Updates

This document presents important content that can be used to assess existing information security and privacy policy libraries to ensure that organizations remain appropriately protected relative to new and emerging risks that emanate from new technologies, operational paradigm shifts, and a continually evolving threat landscape.

NOTE: The dozen or so topics covered in this security policy supplement represent possible gaps that may exist between what is needed and what is specified in current organizational cybersecurity policies. In some instances, the organization may simply need to clarify that existing policies are intended to apply equally to these new use cases. In other cases, new wholesale policies must be established along with related underlying processes, protocols, and in some cases technologies. What is important is that the organization evaluates the degree to which these scenarios apply, assesses the potential impact on its cybersecurity risk exposure, and updates policies assuring the sufficiency of programmatic coverage.

1. Operations Technology (OT) & Internet of Things (IoT)

Topic Description:

With the increasing number of IoT devices being connected to the internet, it's essential to have cybersecurity policies that address the unique security challenges posed by these devices, such as default passwords and unpatched firmware vulnerabilities. Organizations also need to address segmentation questions relative to containment of inbound attacks using OT as an access point to then move horizontally to the data network. Care too must be paid to ensure that scans do not inadvertently "lock" things up, and of course, related to this is the means by which an organization's OT stack is supported by vendors who need remote access.

Policy Discussion:

Operations Technology (OT) typically refers to the hardware and software systems used in industrial control systems, such as those found in manufacturing plants, power plants, and transportation systems.

Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity, allowing them to collect and exchange data over the internet. In simple terms, IoT enables devices to communicate with each other and with humans, creating a vast ecosystem of interconnected objects.

Firmware refers to a type of software that is embedded in non-volatile memory within electronic devices. It provides instructions and control code that enable the device to perform specific functions and operations. Firmware is responsible for managing the hardware components and facilitating the interaction between the hardware and higher-level software or operating systems.

© 2023 The vCISO. All rights reserved

What the three technologies listed above have in common is that they are not typically included in the organization's definition of Information Technology (IT). However, in all of the above cases, these non-IT technologies can create, process, transmit, and/or retain information that must be protected in accordance with its sensitivity and criticality. Consider the following list of devices:

- **Industrial Control Systems (ICS)** – These devices include Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), and Supervisory Control and Data Acquisition (SCADA) systems used to monitor and control industrial processes.

- **Smart Sensors** – Various sensors are deployed in industrial environments to measure parameters such as temperature, pressure, humidity, flow rate, and vibration. These sensors provide real-time data for monitoring and decision-making.

- **Smart Meters** – Used extensively but not exclusively by utility companies, smart meters collect and transmit data related to electricity, gas, or water consumption, enabling accurate billing and better resource management.

- **Building Automation Systems (BAS)** – BAS devices control and monitor building functions such as lighting, heating, ventilation, air conditioning (HVAC), access control, and security systems, allowing for centralized management and improved energy efficiency.

- **Connected Medical Devices** – Healthcare organizations employ various IoT devices such as patient monitoring systems, infusion pumps, wearable health trackers, and remote diagnostic tools to enhance patient care and enable remote monitoring.

- **Connected Vehicles** – Fleet management systems, telematics devices, and connected cars are examples of IoT devices used in the transportation industry to track vehicles, optimize routes, and gather vehicle performance data.

- **Smart Grid Infrastructure** – IoT devices are deployed in power distribution systems to monitor grid performance, detect faults, and enable demand response programs for efficient energy management.

- **Environmental Monitoring Systems** – Sensors and devices are used to monitor air quality, water quality, noise levels, and other environmental parameters in industries, cities, and natural habitats.

- **Asset Tracking and Inventory Management Systems** – RFID tags, GPS trackers, and other IoT devices are used for asset tracking and inventory management in warehouses, logistics, and supply chain operations.

- **Agricultural IoT** – Sensors, weather stations, and automated irrigation systems are employed in precision agriculture to monitor soil conditions, crop health, and optimize resource usage.

© 2023 The vCISO. All rights reserved

All of the above fit within most definitions of OT. But what about the following items:

- Wireless Access Point
- IP Surveillance Camera
- Badge Printers or Badge Readers
- Conference Room Smart Display Monitors

Are these IT devices or OT devices? Candidly, it doesn't really matter how these assets are categorized, the point is that ALL of them need to be included within the scope of an organization's security program. In fact, prudent organizations already understand that security controls must be applied wherever the need to protect information exists. This means that in addition to covering Information Technology, Operations Technology (OT) (i.e., any of the various versions of internet of things) must also be included with the scope to which existing policies, procedures and controls should extend by default. In many cases, however, organizations seemingly unaware of their exposure, fail to apply even the most basic cyber hygiene to these devices. Admittedly, the historic lack of tooling to address OT requirements around access credentials, patching, and basic configurations is a contributing factor. But this is not an acceptable defense, and such devices must be given the same scrutiny and careful consideration relative to the need for legitimate use cases prior to adoption and/or interconnection with the organization's domain.

As with all information assets, organizations should develop, apply, and monitor for drift from established hardening standards, particularly with respect to default credentials, remote access, and communication ports. Generally speaking, it is prudent to segment xIoT devices to the greatest extent possible allowing for a select, few, managed gateways interconnecting with the data network. Such devices should be evaluated for vulnerabilities and such weaknesses should be addressed regularly and in accordance with defined service levels. To the degree that legacy (i.e., EOL) firmware devices must still be used, monitoring must exist to provide a defensible basis for continued use until said items can be replaced or removed.

Guidance:
Considerations for using Operations Technology (OT):

- **Increased Efficiency** – OT can improve operational efficiency, productivity, and automation in industrial processes. OT also enables real-time monitoring, control, and data analysis, allowing for better decision-making and optimization of operations.

- **Enhanced Connectivity** – Integrating OT with IT systems enables data sharing, remote access, and centralized management. This connectivity can improve coordination and collaboration between different departments and facilitate remote monitoring and maintenance.

- **Improved Decision-making** – OT systems provide valuable insights and data analytics that can be used to make informed decisions and optimize processes. Real-time monitoring and analysis can help detect anomalies, predict failures, and implement preventive measures.

© 2023 The vCISO. All rights reserved

- **Cost Reduction** – OT can help streamline operations, reduce manual labor, and minimize downtime. By automating processes, organizations can potentially save costs associated with human error and operational inefficiencies.

Cybersecurity Considerations against using Operations Technology (OT):

- **Increased Attack Surface** – OT systems often operate critical infrastructure and are attractive targets for cybercriminals. The integration of OT with IT networks can expand the attack surface, making it more challenging to defend against cyber threats.

- **Legacy Systems** – Many OT systems have been in use for several years and may have outdated or unsupported software and hardware. These legacy systems may lack the necessary security features and are more vulnerable to cyber-attacks.

- **Lack of Security Awareness** – Operators and personnel involved in OT systems, although well versed and extensively experienced in non-IT operations, frequently have limited cybersecurity knowledge and awareness. This can lead to an increased likelihood of human error (e.g., falling victim to social engineering attacks), improper handling, and/or failing to follow security best practices.

- **Potential Impact of Attacks** – Attacks on OT systems can have severe consequences, including physical damage, operational disruptions, environmental hazards, and potential harm to human life. The potential impact of a successful attack on OT infrastructure requires robust security measures and contingency plans.

- **Difficulty in Patching and Updating** – OT systems often have stringent operational requirements and may not support frequent patching and updates. This can create vulnerabilities and delays in implementing critical security patches, leaving systems exposed to known vulnerabilities for extended periods. And this presumes that the manufacturers of these OT devices agree to be held accountable for these weaknesses, are actively assessing their products for vulnerabilities, and issuing updates/patches.

To mitigate these cybersecurity considerations, organizations should implement robust security measures when adopting OT systems. These measures include:

- **Network Segmentation** – To the degree that organizations can physically separate their OT networks from IT networks they should consider doing so. Nothing is more effective at limiting unwanted traffic than a so-called "airwall". In those situations where physical separation is problematic, organizations should consider logical means of segmentation (i.e., using firewalls and access controls to limit the lateral movement of threats).

- **Regular Security Assessments** – Organizations not yet doing so should embark on a regular and recurring campaign of security assessments. Organizations already doing so must expand the scope of these security assessments and audits to identify vulnerabilities, prioritize risks, and develop

© 2023 The vCISO. All rights reserved

appropriate countermeasures for OT weaknesses (i.e., firmware vulnerabilities) in addition to those related to hardware and software.

- **Defense-in-Depth** – Organizations should consider implementing layered security controls, including firewalls, intrusion detection systems (IDS), encryption, and access controls, to protect OT systems from various attack vectors. This is particularly useful in situations where vendor updates/patches do not exist or will not be immediately forthcoming.

- **Security Awareness Training** – As is the case with all examples of information asset use within an organization, educating personnel about cybersecurity risks, best practices, and incident response procedures is critical to improve overall security posture. Existing security awareness and training content must therefore be expanded to cover the expanded OT footprint, additional use cases, and corresponding standards and protocols.

- **Secure Remote Access** – It is frequently the case that organizations rely upon their OT vendor or Value-Added Reseller (VAR) for support and maintenance of the OT assets acquired and installed on and/or interconnected with the company domain. To this end, companies must ensure that said remote personnel access the company assets in a secure and strictly controlled manner. To this end, organizations may wish to consider implementing secure remote access solutions that employ multi-factor authentication, encrypted connections, and stringent access controls to protect against unauthorized access.

- **Patch Management** – Akin to programs for IT asset management, organizations should establish a process for timely patching and updating of OT systems while considering operational requirements and minimizing disruption. Likewise, organizations may also need to update complimentary standards related to this (e.g., variance approval criteria, risk acceptance authorizations, time bounds, sandboxing requirements, etc.) to account for legitimate differences between OT and IT assets.

- **Incident Response and Business Continuity** – Finally, organizations should review their resiliency plans developing and/or expanding upon their related incident response plan and business continuity capabilities specific to recognize and foster greater resilience with respect to critical dependencies on OT systems minimizing the impact of potential cyber incidents.

By carefully addressing these considerations and implementing appropriate security measures, organizations can leverage the benefits of OT while safeguarding critical infrastructure and systems from cyber threats.

References

The following real-world examples are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- **Honda Ekans** – This Ekans cyberattack (which is snake spelled backwards) affected Honda manufacturing plants which were taken offline secondary to a ransomware attack, wherein bad actors. This event is unusual because organizations are normally concerned about weaknesses in OT devices leading to a compromise of their data network. In this case it would appear that email was the primary

© 2023 The vCISO. All rights reserved

attack vector and that a specifically customized version of the malware in question targeted Honda's production plants/operations.

- **Verkada Hack** – This event refers to the hack of a cloud-based security camera services company infrastructure using a username and password credential pair found publicly on the internet. The bad actors were able to access the company network, including root access to more than 150,000 cameras themselves, which, in turn, enabled unauthorized access to the internal networks of customers. This example not only underscores the need for Third Party Risk Management (TPRM) components in a company cybersecurity program, but also the importance of incorporating OT assets within the scope of applicability. Bottom line, when an organization decides to purchase a cloud-based managed device, whether it be a camera or a printer, the expectation is that the device is a camera or a printer, not a network sniffer with a hot microphone in a room that exfiltrates data and launches attacks.
- **SolarWinds** – This attack was a highly sophisticated intrusion event that leveraged the Orion commercial network performance monitoring software application/platform produced and sold by SolarWinds. Although there are important lessons to be learned by exploring how bad actors were able to compromise SolarWinds, what is significant is that this was a software supply chain attack in which hackers used the company's update server to automatically distribute trojanized software updates to SolarWind's unwitting customers. This points to the critical need organizations have to validate both the source and content of software updates prior to deployment.
- **Dyn DNS DDOS** – Remember when the internet went down, or more precisely when requests for websites could not resolve because the internet "phone book" was being inundated by the Mirai Botnet which infected thousands of OT devices (i.e., distinct from the more traditional botnets comprised of computers) with malware. This sounds highly technical, but it wasn't sophisticated at all, the malware gained unauthorized access by logging in with default passwords! This attack involved three consecutive Distributed Denial of Service (DDOS) attacks launched against the Domain Name System (DNS) provider Dyn. This attack caused major internet platforms and services to be unavailable in what was one of the largest outages of its kind.

Lastly, although no products or vendors are endorsed or otherwise deemed fit for use in a given situation, organizations may wish to explore the following solutions to help address the risks associated with this topic:

- Defender for IoT – Defender for IoT now offers Microsoft customers security for OT environments via the cloud, across all OT devices and sites. This tool is worth consideration, especially for existing Microsoft E3 and E5 customers with a Microsoft-First strategy. As of this writing, Defender for IoT however, is limited to threat detection, and organizations must still address remediation by other means.

- Phosphorous – This is an example of a vendor with an alternative/more comprehensive approach. Like other tools, this offering enables organizations to safely discover, categorize, assess, and manually or automatically remediate OT vulnerabilities.

© 2023 The vCISO. All rights reserved

2. Artificial Intelligence & Machine Learning

Topic Description:

Artificial Intelligence (AI) and Machine Learning (ML) are becoming increasingly prevalent in many industries, and as such, it's essential to ensure that the algorithms and data sets used are secure and protected from cyber threats. Some organizations are evaluating whether to fully or partially block or embrace ChatGPT for example. This is probably an ask for commentary more so than a policy one way or the other as AI can be compared to a pair of scissors. Scissors can be used to make a wonderful craft project with the kids, or they can be used to stab someone in the neck. The tool is not the issue, the question is how it is used.

Policy Discussion

In all but the most restrictive environments, it will be almost impossible to avoid such technology going forward. Therefore, as discussed below, organizations will likely need to develop policies to tightly govern rather than strictly prohibit the use of this technology. But where a desire to block exists, boundary devices, IDS/IPS, URL filtering, and blocklisting technologies can all be leveraged to preclude use. And for many organizations a default block policy with allowable exceptions granted for legitimate use cases may be the right answer. But the organization must be mindful of and fully tolerant of the resulting impact on productivity and utility (e.g., said technology is now embedded in the dominant search engines that may need to be blocked as well). Just as there is a demand for products like Duck Duck Go which are more respectful of organizational privacy concerns, new alternative offerings may emerge but until such time, there may be few options. Relative to acquisition and deployment of said technologies internally, existing change management and TPRM/Vendor management protocols should be followed with Security Impact Assessments (SIAs) conducted pursuant to risk-based decisions. It is highly recommended that all such instances be subject to testing in sandboxed environments until the behavior of the item is well understood, particularly with respect to what data is captured and/or retained, what algorithms are used, and how they operate. Likewise, organizations would do well to recall that we "pay" for such applications one way or the other, either with money or with data – therefore it is prudent to use the paid version instead. Lastly, it is essential to firewall such items off from the public network by default, only allowing external interconnections on a known/good basis. All other applicable security controls (access control, logging, monitoring, patching, hardening, etc.) should be applied.]

Guidance:

When it comes to the use of AI, organizations should consider implementing cybersecurity best practices and policies to ensure the security and integrity of AI systems and the protection of sensitive data. Building on the organization's top-level policy on AI, the following topics offer guidance with respect more implementation standards and other more granular level protocols:

- **Secure AI Model Development** – Organizations should follow secure software development practices when creating AI models. This includes conducting security reviews and assessments throughout the development lifecycle, implementing secure coding practices, and ensuring that AI models are not vulnerable to adversarial attacks or data poisoning.

© 2023 The vCISO. All rights reserved

- **Data Privacy & Protection** – AI systems often rely on large language models and/or other vast quantities of data for both training purposes and live operation. Organizations therefore should establish policies and practices to protect the privacy and integrity of data, including data classification, encryption, and access controls. Compliance with relevant data protection regulations, such as the General Data Protection Regulation (GDPR), should also be ensured by using available opt-in / opt-out provisions and other such settings available within the AI platforms themselves, or where such controls are absent, by implementing supplemental controls independent of the AI solution.

- **Robust Authentication & Access Controls** – AI systems may contain sensitive or proprietary information, and access to these systems should be strictly controlled. Implementing strong authentication mechanisms, such as multi-factor authentication (MFA), and role-based access controls (RBAC), helps prevent unauthorized access to AI systems and their underlying data.

- **Model Validation & Testing** – Organizations should establish processes for testing and validating AI models to ensure their reliability and security. This includes conducting rigorous testing for vulnerabilities, biases, and unintended consequences. Independent audits and third-party assessments can provide valuable insights into the security and performance of AI systems.

- **Explainability & Transparency** – AI systems can sometimes be considered as "black boxes" due to their complex algorithms and decision-making processes. Organizations should strive for transparency and explainability in AI systems, especially in critical use cases. This can help identify potential biases, mitigate risks, and enhance trustworthiness.

- **Ongoing Monitoring & Threat Intelligence** – AI systems should be continuously monitored for potential security threats and vulnerabilities. Implementing security monitoring tools, threat intelligence feeds, and anomaly detection mechanisms will help organizations identify and respond to any suspicious activities or attacks in a timely manner.

- **Human Oversight & Control** – Although AI systems can automate various tasks, it is important to maintain human oversight and control. Humans should be involved in monitoring AI outputs, verifying the system's accuracy, and intervening if necessary. Clear policies and procedures should be established to ensure human accountability and responsibility.

- **Vendor & Supply Chain Management** – If organizations procure AI systems or services from third-party vendors, it is important to assess the security practices of these vendors. This includes evaluating their security controls, conducting due diligence, and establishing clear contractual agreements regarding security responsibilities.

- **Incident Response & Recovery** – Organizations should have robust incident response plans specifically tailored for AI-related incidents. This includes defining roles and responsibilities, establishing communication channels, and having procedures in place to address AI-specific threats such as adversarial attacks or model vulnerabilities.

© 2023 The vCISO. All rights reserved

- **Employee Training & Awareness** – Building a strong cybersecurity culture within the organization is crucial. Regular cybersecurity training and awareness programs should be provided to employees to educate them about potential risks associated with AI systems and promote responsible AI usage.

By implementing these cybersecurity best practices and policies, organizations can minimize the risks associated with AI systems, protect sensitive data, and ensure the reliability and security of their AI deployments. It is important to adapt these practices to specific use cases and stay updated with emerging security challenges in the field of AI.

References:
An abundance of online articles has recently been published as concerns over AI surface. As with most other security decisions, the question about AI is one of risk, ensuring that the organization has a full awareness of its possible exposures and is able to reach a conclusion that the potential benefit to be realized outweighs the possible harm. Two useful articles, including one specific to the recent data breach reported by ChatGPT follow below:

- ChatGPT Confirms Data Breach, Raising Security Concerns (securityintelligence.com)
- 5 Reasons Business Leaders Should Think Twice About ChatGPT (awarehq.com)

NOTE: Organizations must exercise great care with respect to decisions to use AI to ensure compliance with applicable laws, especially when leveraging AI tools for "automated decision making." To this end readers may wish to review this article concerning Brazil's forthcoming legislation related to transparency of algorithms.

© 2023 The vCISO. All rights reserved

3. Cloud Computing & Shared Public Infrastructure

Topic Description:

Cloud computing in one form or another has been around since the 1960's, has been widely adopted by organizations since then, and is now a ubiquitous way for businesses to store and access their data and run their operations. Widespread adoption in the current sense of the cloud, however, did not occur until the mid to late 2000's with many information security practitioners immediately rejecting the idea owing to substantial concerns about the lack of cybersecurity controls. And said professionals were right to be concerned because most cloud providers did not anticipate or provide the same level of security coverage or maturity that leading organizations had themselves. Gradually however, the cloud providers began to recognize the revenue potential in customer concerns over security and expanded their offerings adding both baked in security as well as customizable options organizations could choose on an ala carte basis.

Not surprisingly however, as long-established organizations began migrating on-premises workloads to the cloud and as newer organizations adopted a cloud-first strategy, the major providers increasingly became targets of attack themselves. This would be problematic by itself, but the situation is made worse by the fact that many organizations fail to appreciate that although they can engage others to host their systems and data, they cannot absolve themselves of responsibility for the security and privacy of their information; it is therefore essential to ensure that proper security measures are in place to protect data stored in the cloud.

Policy Discussion:

Cloud computing offers tremendous benefits and economies of scale. And for many small to mid-size organizations, the dominant CSPs can deliver better and more capable security controls that most organizations can afford to acquire, configure, deploy, and maintain on their own. However, for the same reason that the internet was created in the first place (i.e., concerns about dependencies on 100% on-prem computing interconnected by long distance telephone lines) organizations should exercise great care not to put all of their compute into the cloud. Cloud providers typically offer strong resiliency but public network outages, power grid issues, DDOS attacks on DNS service providers, and other such issues demand that organizations develop and maintain alternative/downtime procedures that all critical operations to be maintained.

Additionally, it is vital to understand that although security fulfillment may be outsourced to the cloud, accountability for the protection of information and compliance with regulations cannot. Further, based on most so-called "shared responsibility models" (think CSA) cloud providers typically are only able to fulfill about 1/3 of the controls in most frameworks (e.g., NIST, ISO) leaving 1/3 up to companies to do entirely for themselves and the remaining 1/3 as things that must be performed jointly with the CSP. Lastly, there are two other items of which to be mindful. First, it may be necessary to impose data localization restrictions on your CSP to ensure that you meet regulatory requirements of certain jurisdictions. Second, organizations may find it prudent to store backup copies of their critical data with a separate cloud provider apart from the one they use to host their production operations.

Guidance

© 2023 The vCISO. All rights reserved

Considerations for Cloud Computing:

- **Data Security** – Organizations must ensure that their data is adequately protected in the cloud. This includes implementing strong access controls, encryption, and data segregation to prevent unauthorized access, data breaches, and data loss.

- **Privacy & Compliance** – When using cloud services, organizations must address privacy concerns and ensure compliance with relevant data protection regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

- **Vendor Security** – Organizations should assess the security practices and reliability of cloud service providers. This includes evaluating their security certifications, data center security measures, incident response capabilities, and contractual obligations for data protection.

- **Shared Responsibility** – Cloud computing involves a shared responsibility model, where the cloud provider is responsible for the security of the cloud infrastructure, while the customer is responsible for securing their applications, data, and access controls. Organizations must understand and fulfill their security responsibilities within the cloud environment.

- **Data Governance** – Effective data governance becomes crucial when leveraging cloud services. Organizations need to have policies and procedures in place to ensure proper data handling, access controls, and data lifecycle management throughout the cloud ecosystem.

- **Service Availability** – Dependence on cloud services means organizations must consider the potential impact of service disruptions or outages. Implementing backup and disaster recovery strategies, redundancy measures, and service level agreements (SLAs) with the cloud provider can help mitigate these risks.

Considerations Against Cloud Computing:

- **Loss of Control** – Entrusting data and services to a cloud provider means relinquishing some control over infrastructure, security measures, and system configurations. Organizations should carefully evaluate their comfort level with this loss of direct administrative control. Also, although many organizations actually seek to transfer these administrative responsibilities to another party to allow themselves to focus on what is core to their business leaving IT in the often more capable hands of vendors, use of the cloud necessitates the expansion of company operations in areas of vendor management and oversight. This trade off may lessen or even completely negate the benefits of going to the cloud.

- **Data Location & Jurisdiction** – Data stored in the cloud may reside in different geographical locations, which raises concerns about data sovereignty and jurisdictional compliance. Organizations should understand where their data is stored and ensure compliance with relevant regulations.

© 2023 The vCISO. All rights reserved

- **Dependency on Internet Connectivity** – Cloud computing heavily relies on internet connectivity. Organizations must consider the potential impact of network outages or disruptions on their ability to access cloud services and critical data. Organizations with critical operations and/or low tolerances for downtime, must invest in resiliency/redundancy to avoid unwanted impacts of extended disruptions.

- **Vendor Lock-In** – Migrating to the cloud may result in dependencies on specific cloud platforms or technologies. It may be challenging to switch providers or transition back to an on-premises infrastructure without significant effort and cost. Organizations must be strategic in their decisions to use cloud vendors readily deploying "commodity" operations by exercising greater caution with respect to their more unique/customized workloads.

- **Insider Threats & Data Breaches** – The cloud introduces additional attack vectors and potential risks for insider threats. Organizations must implement robust access controls, monitor user activities, and implement security measures to detect and prevent unauthorized access or data breaches.

- **Compliance Challenges** – Meeting industry-specific regulatory requirements or internal compliance policies can be more complex in a cloud environment. Organizations must work closely with cloud providers to ensure compliance and maintain necessary audit trails.

It is important for organizations to conduct a comprehensive risk assessment, evaluate their specific security requirements, and implement appropriate security controls when considering the use of cloud computing. By understanding and addressing these cybersecurity considerations, organizations can make informed decisions and mitigate potential risks associated with cloud adoption.

References

In all but the rarest and most demanding of situations, it is hard to imagine a business reaching a conclusion to completely avoid use of the cloud. What is vital is for leadership to understand and weigh the pros and cons and make a fully informed decision. To this, end, organizations would do well to remember, that according to one recent study conducted by Thales, 45% of all organizations surveyed experienced a data breach or failed an audit involving data and applications in the cloud and further, this was up from 35% who reported the same negative outcomes the prior year in 2021.

Upon reflection, such outcomes are not that surprising as bad actors frequently target the large Cloud Service Providers (CSPs) often finding success because of the unclear delineation of security responsibilities between host and customer along with failures by customers to harden their environments appropriate. Examples of some of the larger cloud based cyber-attacks include:

- Accenture suffered a data breach involving confidential API data, digital certificate, decryption keys, meta information, and user data after leaving four AWS S3 storage buckets unsecured.

- In 2017, Verizon's third-party cohort, Nice Systems, erroneously exposed user PPI due to a faulty AWS S3 configuration. The attack was made possible due to Nice's error that further collected customer call data.

© 2023 The vCISO. All rights reserved

- IT solutions provider Kaseya suffered a massive attack on their unified remote monitoring and network perimeter security tool.

- Cybersecurity analytics giant Cognyte made a blunder leaving their database unsecured without authentication protocols. This folly paved the way for cyber-attackers, exposing 5 billion user records.

© 2023 The vCISO. All rights reserved

4. Quantum Computing

Topic Description:

Quantum computing is an emerging field of computing that harnesses the principles of quantum mechanics to process information in a fundamentally different way than classical computers. While classical computers use bits as the basic unit of information, which can represent either a 0 or a 1, quantum computers use quantum bits, or qubits, which can exist in a superposition of states, representing both 0 and 1 simultaneously. This ability to be in multiple states simultaneously is what gives quantum computers their potential for exponential computational power. By manipulating and entangling qubits, quantum computers can perform parallel computations and solve certain problems much faster than classical computers. Quantum computing has the potential to revolutionize various fields such as cryptography, optimization, drug discovery, and materials science.

Although, still in its early stages, quantum computing has the potential to revolutionize many industries. However, it also poses a significant cybersecurity threat, as quantum computers could potentially break many of the encryption algorithms currently in use. There are also rumblings about legacy encryption technologies and embedded "flaws" that may be included "by design" to enable governments to better fulfill their national security missions.

Policy Discussion:

Quantum computing has the potential to break many of the cryptographic algorithms currently used to secure data, including asymmetric encryption, digital signatures, and key exchange protocols. This raises the need for developing and implementing quantum-resistant encryption algorithms, often referred to as Post-Quantum Cryptography (PQC). Transitioning to PQC algorithms is crucial to ensure the long-term security of sensitive data.

This is in many ways an industry-wide concern that is not unique to any one organization. However, organizations cannot simply ignore the problem. Instead, they should include this topic in their regular recurring risk assessments and develop strategies for transitioning to post-quantum crypto as such capabilities emerge.

Guidance:

Considerations for using quantum computing:

- **Advanced Threat Landscape** – Quantum computing could empower attackers with unprecedented computational capabilities, enabling them to break encryption, crack passwords, or solve complex mathematical problems much faster than classical computers. Organizations need to anticipate these advanced threats and proactively develop countermeasures to safeguard their systems and data.

- **Quantum Key Distribution (QKD)** – Quantum computing also offers the potential for secure communication through quantum key distribution. QKD leverages quantum principles to establish secure encryption keys, ensuring that any interception or eavesdropping attempt is detectable.

© 2023 The vCISO. All rights reserved

Implementing QKD protocols can enhance the security of data in transit and mitigate the risk of key compromise.

- **Enhanced Simulations & Threat Modeling** – Quantum computing can improve simulations and modeling techniques, enabling better understanding and prediction of cyber threats. This capability can assist in identifying vulnerabilities, testing defenses, and enhancing incident response strategies.

Considerations against using quantum computing:

- **Breaking Current Encryption** – The most significant concern related to quantum computing is its potential to break widely used cryptographic algorithms. Many encryption protocols that currently protect sensitive data and secure communications would become vulnerable to quantum attacks. Organizations relying on these algorithms will need to transition to quantum-resistant cryptography to ensure data confidentiality and integrity.

- **Data-At-Rest Security** – Quantum computing can also compromise the security of data stored in various forms, such as encrypted databases or files. Even if data is encrypted using classical encryption methods, quantum computers could potentially decrypt the data by breaking the encryption algorithms. This highlights the need to adopt quantum-resistant encryption algorithms and migrate sensitive data to post-quantum secure formats.

- **Quantum-Based Attacks** – As quantum computing progresses, new attack techniques leveraging quantum principles may emerge. This could include novel methods for cryptanalysis, sophisticated quantum-based side-channel attacks, or exploitation of vulnerabilities in quantum computer hardware. Organizations will need to adapt their security strategies to address these emerging threats and stay ahead of potential attackers.

- **Quantum Computer Availability** – Although quantum computing is advancing, practical and scalable quantum computers that pose a significant threat to classical cryptography are not yet widely available. However, the timeline for when such machines may become accessible remains uncertain. Organizations need to monitor developments in quantum computing and be prepared to adapt their security measures accordingly.

- **Transition Challenges** – The transition from classical to post-quantum cryptography can be complex and resource-intensive. It requires updating systems, protocols, and cryptographic libraries across various platforms, including hardware, software, and network infrastructure. Organizations must carefully plan and execute this transition to ensure a smooth migration to quantum-resistant algorithms without compromising security.

In summary, quantum computing offers significant opportunities but also poses challenges to cybersecurity. Organizations should proactively assess the impact of quantum computing on their security posture, invest in quantum-resistant cryptography, and stay informed about advancements in the field to adapt their security strategies as needed.

© 2023 The vCISO. All rights reserved

References

As of this writing, I am not aware of any actual breaches officially attributed to quantum computing (either owing to limitations in the technology or as a result of its advanced capabilities). Readers interested in exploring the topic further are encouraged to review the following sources and/or follow these organizations:

- IBM Quantum and UC Berkely – As one of the foremost leaders in the space, IBM is at the forefront of this topic and has research and reports related to the fulfillment of cybersecurity objectives in the era of quantum computing.

- World Economic Forum – Provides useful guidance and cautionary tales concerning the use of quantum computing along with recommendations for the adoption of "safe" strategies and pursuits.

- DHS / NIST – The Department of Homeland Security (DHS), in partnership with the Department of Commerce's National Institute of Standards and Technology (NIST), released a roadmap to help organizations protect their data and systems and to reduce risks related to the advancement of quantum computing technology.

© 2023 The vCISO. All rights reserved

5. Blockchain Technology

Topic Description:

Blockchain technology is a decentralized and transparent system that uses cryptography to securely record and verify transactions. It eliminates the need for intermediaries and central authorities, ensuring integrity and reducing the risk of manipulation. By maintaining a distributed ledger across a network of computers, blockchain theoretically enables secure and tamper-resistant data storage, offering potential applications in various industries beyond cryptocurrencies. Consequently, blockchain technology has become increasingly popular in recent years. However, it is important to ensure that the security measures used to protect blockchain networks are robust and able to withstand cyber-attacks.

Policy Discussion

When evaluating the possible use of blockchain technology, it is important to be mindful of certain cybersecurity considerations. Although blockchain offers certain security benefits, it is not impervious to risks and vulnerabilities. Further, this is an example of where the company likely has many of the necessary cybersecurity policies already in place and must simply expand the scope of applicability to incorporate blockchain as discussed below:

- **Expanded Cybersecurity Policy** – The organization should expand its policy specifically addressing the security aspects of blockchain technology. Presuming that the technology is not outlawed outright, this policy should cover guidelines for secure implementation, access controls, encryption, secure coding practices, and incident response procedures.

- **Access Control & Identity Management** – Implement strict access controls and identity management practices for blockchain networks. This includes strong authentication mechanisms, role-based access controls, and the principle of least privilege to ensure that only authorized individuals can access and interact with the blockchain.

- **Secure Smart Contract Development** – Smart Contracts refer to self-executing agreements with the terms of the contract directly written into code and stored on a blockchain. Secure smart contracts aim to prevent or minimize potential exploits, vulnerabilities, and unintended consequences that can arise from coding errors or malicious activities. In support of their use however, organizations must establish policies and procedures for secure smart contract development. This should include code review processes, testing methodologies, and adherence to best practices for writing secure smart contracts to minimize the risk of vulnerabilities and exploits.

- **Data Privacy & Compliance** – Organizations should review and revise their policies to address privacy concerns related to blockchain technology ensuring compliance with data protection regulations, such as GDPR or CCPA. Organizations may also wish to consider implementing privacy-enhancing techniques, data anonymization, and appropriate consent mechanisms.

© 2023 The vCISO. All rights reserved

- **Incident Response & Recovery** – Organizations should review and revise their resiliency capabilities updating their Incident Response Plan (IRP) specifically for blockchain-related incidents. This plan should outline procedures and contain playbooks for detecting and responding to security breaches, as well as strategies for recovering from attacks or disruptions in the blockchain network.

- **Third-Party Risk Management** – Establish policies and guidelines for engaging with third-party blockchain service providers or partners. Conduct due diligence assessments to evaluate the security practices, reliability, and reputation of third-party vendors before integrating their services or solutions.

- **Regular Security Audits & Assessments** – Implement regular security audits and assessments to identify vulnerabilities, assess risks, and ensure compliance with security policies. Regularly evaluate the blockchain infrastructure, smart contracts, and associated systems for potential weaknesses or misconfigurations.

- **Employee Training & Awareness** – Promote cybersecurity awareness and provide regular training to employees on the secure use of blockchain technology. Educate employees about the risks, best practices, and security policies relevant to blockchain to ensure their responsible use and adherence to security guidelines.

- **Monitoring & Logging** – Implement monitoring mechanisms to detect and analyze suspicious activities within the blockchain network. Maintain logs and audit trails of transactions, events, and system activities to facilitate forensic investigations and facilitate compliance requirements.

- **Secure Key Management** – Establish policies and procedures for secure key management, including private keys used for digital signatures or access controls within the blockchain network. Implement best practices for key generation, storage, backup, and rotation to prevent unauthorized access or loss of keys.

Guidance

Considerations for Blockchain Technology:

- **Data Integrity & Immutability** – Blockchain provides tamper-resistant and immutable data storage, ensuring that once information is recorded on the blockchain, it is challenging to alter or manipulate. This feature enhances data integrity and can be beneficial for applications requiring secure and auditable records.

- **Distributed & Decentralized Architecture** – Blockchain's distributed nature reduces the risk of a single point of failure and increases resilience against attacks. The decentralized consensus mechanism makes it difficult for adversaries to compromise the entire network.

- **Cryptographic Security** – Blockchain employs cryptographic algorithms to secure data and transactions. Strong encryption and hashing algorithms are used to protect data confidentiality, integrity, and authenticity within the blockchain network.

© 2023 The vCISO. All rights reserved

- **Smart Contract Security** – Smart contracts, which are self-executing agreements on the blockchain, introduce their security considerations. Auditing and thoroughly testing smart contracts for vulnerabilities is crucial to prevent exploits, code vulnerabilities, or unintended consequences.

- **Transparency & Auditability** – The transparent nature of blockchain enables participants to validate and audit transactions. This transparency can improve trust, accountability, and provide transparency in supply chains, financial transactions, and voting systems.

Considerations Against Blockchain Technology:

- **Scalability & Performance** – Blockchain's distributed nature and consensus mechanisms can result in limited scalability and performance issues. As the size of the blockchain grows, transaction processing times may increase, leading to potential bottlenecks.

- **Governance & Legal Challenges** – Blockchain governance, including decision-making, consensus protocols, and updates, can be complex. Establishing effective governance structures, resolving disputes, and adapting to legal frameworks can present challenges in certain use cases.

- **Privacy Concerns** – Blockchain's transparent and immutable nature can conflict with privacy requirements, especially for sensitive or personally identifiable information. Organizations must carefully design blockchain solutions and consider privacy-enhancing techniques like zero-knowledge proofs or off-chain data storage.

- **Smart Contract Vulnerabilities** – Although smart contracts offer automation and efficiency, they can also introduce security risks. Vulnerabilities in smart contracts may lead to exploits, theft, or unintended consequences. Thorough code reviews, security audits, and best practices for secure development are crucial.

- **Complexity & Skill Requirements** – Blockchain technology is relatively complex, requiring specialized knowledge and expertise. Implementing and maintaining blockchain systems may require skilled professionals who understand the intricacies of blockchain security and can address potential vulnerabilities effectively.

- **Regulatory & Compliance Challenges** – Blockchain adoption can be influenced by regulatory uncertainty and compliance requirements. Organizations must navigate evolving legal and regulatory landscapes, ensuring compliance with data protection, financial regulations, and other relevant laws.

It is essential for organizations to evaluate the specific requirements, use cases, and potential risks associated with blockchain technology. Thoroughly understanding the cybersecurity considerations allows organizations to implement appropriate security measures, address potential vulnerabilities, and leverage the benefits of blockchain technology effectively.

References

© 2023 The vCISO. All rights reserved

The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- Basic Blockchain Security -- Blockchain security is a comprehensive risk management system for a blockchain network, using cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and fraud. Review this article from IBM for details.

- $1.9 Billion Stolen in crypto in 2022 – A staggering $1.9 billion worth of cryptocurrency was stolen in hacks of various services in the first seven months of 2022, marking a 60% increase from the same period in the year prior, according to a report released from blockchain analysis firm Chainalysis.

- $100 million worth of crypto hacked – Hackers have stolen $100 million in cryptocurrency from Horizon, a so-called blockchain bridge, in the latest major heist in the world of decentralized finance.

- Top Blockchain Attacks, Hacks, and Security Issues Explained – Despite the presence and continued application of security enhancements, the blockchain market has been plagued with security issues from blockchain specific attacks to human vulnerabilities as described in this article.

© 2023 The vCISO. All rights reserved

6. 5G Networks / Smart City Infrastructure

Topic Description:

5G networks refer to the fifth generation of wireless technology, offering significant advancements over previous generations (4G, 3G, etc.). 5G provides faster and more reliable connectivity, lower latency, and increased capacity to support a wide range of devices and applications. 5G networks employ advanced technologies such as higher frequency bands, massive MIMO (Multiple-Input Multiple-Output), and beamforming to deliver faster data speeds and improved network performance. It enables transformative capabilities like ultra-high-definition video streaming, virtual and augmented reality, autonomous vehicles, Internet of Things (IoT) devices, and smart city infrastructure. With its high data transfer rates, low latency, and massive device connectivity, 5G has the potential to revolutionize various industries and drive innovation across sectors. However, 5G networks also pose new cybersecurity challenges so it is essential to ensure that 5G networks are secure and protected from cyber threats.

Policy Discussion

5G networks bring numerous benefits such as higher speeds, lower latency, and increased capacity, but they also introduce unique cybersecurity considerations. As is the case with all types of technologies, organizations must decide whether these benefits outweigh the risks and then govern use of 5G networks accordingly. To this end, organizations should update their security policies and guidelines to outline the acceptable use of 5G networks, specifying the types of activities that are allowed and/or prohibited, what data handling protocols are to be observed, what device security configurations/controls are required, and what restrictions or limitations apply to network usage.

For security minded organizations with established protocols concerning the use of public wireless networks, the advent of 5G networks need not significantly add to the overall risk posture. For example, if users are already trained to confirm the name of an SSID with establishment personnel if the necessary information is not prominently posted, then it should be easy to pivot to allow use of Smart City Infrastructure. Conversely if your personnel are allowed to use insecure public Wi-Fi hotspots and do so without verifying authenticity, then the move to 5G will substantially increase the likelihood of compromise by man-in the middle attacks.

NOTE: It is somewhat beyond the scope of this document, but organizations would do well to consider the source of 5G infrastructure equipment when considering their policies. To the degree that concern exists relative to computing equipment manufactured outside the US organizations should expand their TPRM and/or supply chain programs accordingly.

Guidance:

Considerations for using 5G networks:

- **Enhanced Attack Surface** – The increased number of connected devices and the broader network coverage of 5G expand the attack surface for cyber threats. More devices and endpoints provide more entry points for potential attacks, increasing the complexity of securing the network.

© 2023 The vCISO. All rights reserved

- **IoT vulnerabilities** – 5G networks are expected to support a massive deployment of Internet of Things (IoT) devices. However, many IoT devices have historically demonstrated security weaknesses, such as default credentials, lack of updates, or poor encryption. The sheer scale and diversity of connected devices in 5G networks can pose challenges for ensuring their security.

- **Network Slicing Risks** – 5G introduces the concept of network slicing, allowing multiple virtual networks to run simultaneously on shared infrastructure. Although network slicing provides flexibility and tailored services, it can also introduce risks if proper isolation between slices is not ensured. Inadequate isolation can enable lateral movement or unauthorized access between different slices, compromising network security.

- **Supply Chain Security** – 5G networks rely on a complex ecosystem involving numerous vendors and suppliers. Securing the supply chain becomes crucial to prevent compromises, such as the insertion of malicious components or software in network infrastructure. Verifying the security practices of vendors, conducting thorough risk assessments, and implementing robust supply chain management processes are essential to mitigate these risks.

- **Mobile Device Vulnerabilities** – With 5G, mobile devices become even more integral to daily activities, including critical business operations. However, mobile devices often face security challenges such as malware, phishing attacks, and data leakage. It is crucial to implement robust mobile device management practices, including secure configurations, regular patching, and user education to mitigate these risks.

Considerations against using 5G networks:

- **Increased Attack Complexity** – The higher speeds and lower latency of 5G networks enable new forms of attacks that were previously not feasible. For example, the lower latency may facilitate faster propagation of malware or enable more effective distributed denial of service (DDoS) attacks. Advanced attacks leveraging the benefits of 5G can pose significant challenges for detection, response, and mitigation.

- **Threats From Emerging Technologies** – 5G enables the adoption of emerging technologies such as edge computing and Internet of Things (IoT). Although these technologies provide new opportunities, they also introduce additional security risks. Edge devices and IoT endpoints may have limited computing resources and security capabilities, making them potential targets for exploitation or compromise.

- **Privacy Concerns** – 5G networks are capable of collecting and processing massive amounts of data due to increased connectivity and network intelligence. This raises concerns about privacy, data protection, and user consent. Collecting and securing such large volumes of sensitive data requires robust privacy policies, encryption mechanisms, and strict access controls to prevent unauthorized disclosure or misuse.

© 2023 The vCISO. All rights reserved

- **Insider Threats** – As the complexity of 5G networks increases, the risk of insider threats also grows. Insiders with privileged access, such as network administrators or employees of service providers, can exploit their positions to compromise network security, disclose sensitive information, or disrupt services. Implementing stringent access controls, monitoring privileged accounts, and conducting regular security audits are essential to mitigate insider threats.

- **National Security Considerations** – The deployment of 5G networks has raised national security concerns, particularly regarding the involvement of foreign vendors and potential risks of backdoors or espionage. Governments and organizations need to carefully evaluate the security implications, conduct risk assessments, and implement appropriate measures to ensure the integrity and security of 5G infrastructure.

In summary, 5G networks offer significant advantages, but they also introduce new cybersecurity considerations. It is essential to address these considerations through a combination of robust security practices, risk assessments, vendor evaluations, user education, and ongoing monitoring to ensure the security and resilience of 5G networks.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- Council on Foreign Relations – Challenges and Recommendations for Securing 5G Networks.

- 5G Security and Resilience – This site presents guidance from the combined forces of the CISA, NSA, and the Director of National Intelligence including materials from the Enduring Security Framework (ESF) a cross-sector, public-private working group.

© 2023 The vCISO. All rights reserved

7. Return to Office (RTO)

Topic Description:

As companies are implementing Return to Office (RTO) programs that compel staff to come back into the office following the lifting of the state of emergency related to the COVID Pandemic, there will inevitably be a meaningful percentage of staff who are either unable or unwilling to do so. Companies need policies regarding whether they can terminate for this reason and if so, what they must do to assure the return of any/all information and information assets that may have been used by personnel working remotely during the pandemic. Also, organizations will need to engage their Human Resources and Legal departments to obtain clarification on whether companies are able to withhold final payroll pending receipt of equipment, especially if the organization did not have personnel sign a care and use form upon originally taking receipt of equipment. Likewise, employers need to be mindful to avoid claims of wrongful/unfair dismissal, particularly if the personnel in question have legitimate claims for "reasonable accommodations." Lastly, there should be some discussion of asset sanitization and/or software removal protocols that need to be followed if organizations choose to allow outgoing personnel to retain equipment (i.e., transferring ownership without putting data at risk or violating software piracy rules).

Policy Discussion

As organizations who have made meaningful investments in cybersecurity already know, it is quite often the case that in developing policies, procedures, and controls to manage information risk, entities uncover broken or missing business processes that may have little or no direct relation to information, but nonetheless represent threats to the business. This is very much the case with what is probably the first decision organizations will need to make with respect to RTO, namely, whether to risk losing valuable knowledge workers by forcing them to return against their wishes.

Many senior organizational leaders hold fast to the belief that staff are unable to collaborate well or be innovative if they are not physically working together in the same space. And in certain industries, companies, or geographies, this may in fact be the case. But in setting an RTO policy, leaders would do well to be mindful that many in their workforce have grown fond of working remotely and may be reluctant to give up the various benefits such an arrangement offers. Remote personnel argue that they are more productive often working longer hours because they do not have to spend time commuting to and from work. Others cite less distractions, greater flexibility, and the all-important work-life balance as reasons they seek the ability to continue working from home. Organizations who do not consider the feelings and preferences of their work force may find that some staff would rather resign than go back to work in an office each day. Rather than an all or nothing policy, organizations may find it advantageous to allow personnel to work from home on certain days of the week/month coming into the office on other times when everyone is together. Likewise, organizations may limit RTO policies to certain job roles/types, especially in industries or positions with severe staffing shortages. Ultimately, some organizations may decide to allow personnel to continue remote work rather than risk the loss of critical personnel and/or knowledge.

To the degree that organizations decide that a post-COVID pandemic return to the office is appropriate, they need to be mindful that cybersecurity policy considerations play a crucial role in ensuring the security and

© 2023 The vCISO. All rights reserved

resilience of the organization's systems and data. Here are some key cybersecurity policy considerations for organizations:

- **Remote Work Transition** – If remote work arrangements were implemented during the pandemic, organizations need to assess the cybersecurity policies and controls that were put in place to support remote work. As personnel return to the office, policies should be reviewed and updated to address any changes in work arrangements, such as hybrid work models or flexible work schedules.

- **Endpoint Security** – Organizations should consider the security of endpoints (e.g., laptops, desktops, mobile devices) that were used for remote work. Ensuring that these devices are updated with the latest security patches, have up-to-date antivirus software, and adhere to security configurations and policies is essential to prevent potential security breaches or malware infections. This is especially true if organizations allowed personnel to use their own equipment during the pandemic but may not wish to adopt a Bring Your Own Device (BYOD) policy with respect to direct connections to the corporate domain (i.e., as opposed to Citrix/VDI for example).

- **Access Controls** – Organizations should review and adjust access controls to align with the return to the office. User accounts and permissions should be reviewed to ensure that employees have appropriate access levels based on their roles and responsibilities. Revoking access for employees who no longer require it and implementing multi-factor authentication (MFA) can enhance security. Similarly, organizations who subject physical and/or logical access controls to automatic inactivity revocations will need to determine who needs to have their privileges reset ahead of time to avoid an upsurge in access issues and/or helpdesk tickets.

- **Network Security** – Organizations should assess and reinforce network security measures to protect office networks and prevent unauthorized access. This may include implementing firewalls, intrusion detection and prevention systems, network segmentation, and secure Wi-Fi networks. Regular network vulnerability assessments and penetration testing can help identify and address potential weaknesses. NOTE: Controls such as these should have been in place both before and throughout the Pandemic but are critical now to ensure that devices that may have been compromised during use by personnel when working from home during do not introduce unwanted risk to the organization upon joining/rejoining the domain.

- **Physical Security** – As employees return to the office, physical security measures should be reviewed and updated. This includes controlling access to office spaces, securing server rooms and critical infrastructure, and implementing video surveillance and alarm systems. Employees should also be educated about physical security practices, such as locking their workstations and reporting suspicious activities. Organizations should do this for all personnel but may wish to focus on personnel hired during the pandemic who did not previously work within company facilities.

- **Employee Training & Awareness** – Organizations should provide cybersecurity training and awareness programs to educate employees about potential risks and best practices. This includes topics such as identifying phishing attempts, safe browsing habits, secure password management, and reporting security incidents. Regularly reinforcing these training initiatives can help create a security-conscious

© 2023 The vCISO. All rights reserved

workforce. Hereto, companies may need to provide additional guidance to personnel hired during the pandemic.

- **Incident Response & Business Continuity** – Organizations should review and update their incident response and business continuity plans to reflect the return to the office. This includes identifying key personnel responsible for cybersecurity incident response, conducting tabletop exercises, and ensuring that backup and recovery procedures are in place to minimize downtime in case of a cybersecurity incident.

- **Compliance & Regulatory Requirements** – Organizations should consider any compliance or regulatory requirements specific to their industry or location. This may include data protection regulations, privacy laws, or industry-specific security standards. Ensuring that cybersecurity policies align with these requirements is essential to avoid legal and regulatory issues.

- **Vendor & Third-Party Risk Management** – Organizations should assess the cybersecurity posture of their vendors and third-party service providers. This includes reviewing contracts and service-level agreements to ensure that appropriate security measures are in place. Regularly monitoring and auditing third-party security practices can help mitigate potential risks.

- **Employee Privacy** – Organizations should balance cybersecurity requirements with employee privacy concerns. Any monitoring or data collection activities should be conducted in compliance with applicable privacy laws and regulations. Transparency and clear communication about privacy practices can help build trust and mitigate privacy-related concerns.

By considering these cybersecurity policy considerations, organizations can establish a strong security foundation as employees return to the office, ensuring the protection of their systems, data, and personnel. It is important to regularly review and update these policies to adapt to evolving cybersecurity threats and changes in the organizational environment.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- How to Overcome Return-to-Office Resistance – Read this Harvard Business Review article for guidance on how best to navigate this challenge with professional and personal implications.

© 2023 The vCISO. All rights reserved

8. Augmented Reality (AR) and Virtual Reality (VR)

Topic Description:

Augmented Reality (AR) and Virtual Reality (VR) are immersive technologies that enhance our perception of the real world or create entirely virtual environments. AR combines computer-generated elements with the real world, overlaying virtual objects or information onto our immediate surroundings. By using cameras, sensors, and display devices like smartphones or smart glasses, AR enhances our perception of reality by adding digital elements such as 3D models, text, or animations onto our view of the physical world. This technology has diverse applications, ranging from gaming and entertainment to education, healthcare, retail, and industrial sectors.

VR provides a fully immersive, computer-generated environment that simulates a user's physical presence in a virtual world. By wearing a VR headset, users are visually and audibly isolated from their physical surroundings, completely immersed in a digital environment that can be entirely computer-generated or based on real-world content. VR allows users to interact with and navigate through this simulated reality, often using handheld controllers or specialized input devices. It is widely used in gaming, training simulations, virtual tours, architectural visualization, and therapeutic applications.

Both AR and VR technologies offer unique experiences and have the potential to transform various industries. While AR enhances the real world with digital information, VR transports users to entirely virtual environments. Both technologies continue to evolve and find new applications as they provide immersive and interactive experiences, blurring the line between the digital and physical realms. AR and VR are becoming more prevalent in industries such as gaming, education, and healthcare. As these technologies become more integrated into our lives, it's important to ensure that they are secure and protected from cyber threats.

Policy Discussion

Augmented Reality (AR) and Virtual Reality (VR) technologies are becoming increasingly popular, transforming various industries and enhancing user experiences. However, their adoption also introduces new cybersecurity considerations. Additionally, in many business situations, AR/VR is an example of a technology in search of a problem to solve. Therefore, it is of paramount importance that organizations evaluate for and ensure alignment between these technologies and their business. Specifically, organizations should assess how AR/VR can align with the organization's goals and objectives. Determine if there are specific areas where AR/VR can enhance productivity, improve training, streamline processes, or enhance customer experiences. Likewise, organizations should consider whether the use of AR/VR aligns with the organization's industry, services, or products. To the degree that the benefits outweigh the risks can and should adopt AR/VR but in doing so must expand their security policies accordingly.

Guidance:

Considerations for using AR and VR:

- **Data Privacy** – AR and VR applications often collect and process significant amounts of user data, such as location information, biometric data, or behavioral patterns. Ensuring robust data privacy

© 2023 The vCISO. All rights reserved

measures, including secure data storage, encryption, and user consent mechanisms, is crucial to protect user privacy.

- **User Safety** – AR and VR experiences typically involve users being immersed in a virtual environment or overlaying digital content on the real world. However, this can sometimes lead to physical risks if users are not fully aware of their surroundings. Educating users about potential safety hazards and implementing appropriate warnings and safety measures is essential.

- **User Authentication** – AR and VR applications may require user authentication to access personalized content or services. Traditional authentication methods like usernames and passwords may not be sufficient. Employing strong authentication mechanisms, such as biometrics or multi-factor authentication, helps prevent unauthorized access to AR and VR systems and associated data.

- **Malware & Phishing** – As AR and VR platforms gain popularity, they become attractive targets for cybercriminals. Malware and phishing attacks can exploit vulnerabilities in software, hardware, or user behaviors. Implementing robust security measures, such as regular software updates, antivirus software, and user education about phishing risks, is vital to mitigate these threats.

- **Device Security** – AR and VR experiences are delivered through a variety of devices, including headsets, smartphones, or wearable devices. These devices may have their own security vulnerabilities that can be exploited. Employing secure configurations, applying patches and updates, and using trusted software sources are essential for maintaining device security.

Considerations against using AR and VR:

- **Social Engineering** – AR and VR experiences often rely on user interactions and engagements. Attackers can exploit this by employing social engineering techniques to manipulate users and trick them into disclosing sensitive information or performing malicious actions. Educating users about potential social engineering tactics and promoting skepticism can help mitigate these risks.

- **Unauthorized Access To Physical Spaces** – AR and VR applications that interact with physical spaces, such as smart home integration or industrial environments, may introduce risks of unauthorized access or control. Implementing strong access controls, encryption, and secure communication protocols is essential to prevent unauthorized manipulation of physical systems.

- **Data Leakage & Exposure** – AR and VR applications may transmit and store sensitive user data. If not properly secured, this data can be vulnerable to unauthorized access or disclosure. Employing encryption, access controls, and secure data transmission protocols are crucial to protect user data and prevent data breaches.

- **Third-Party Vulnerabilities** – AR and VR applications often rely on third-party software libraries, frameworks, or content repositories. These dependencies may introduce security vulnerabilities if not properly vetted. Conducting thorough security assessments of third-party components and regularly updating and patching them is important to mitigate these risks.

© 2023 The vCISO. All rights reserved

- **Lack Of Industry Standards** – As AR and VR technologies continue to evolve rapidly, the lack of standardized security practices and frameworks can pose challenges. Organizations adopting AR and VR should stay informed about emerging security standards, participate in industry collaborations, and work towards establishing best practices to ensure a secure environment.

In summary, AR and VR technologies offer exciting possibilities but also require careful attention to cybersecurity. By addressing these considerations, implementing strong security measures, and promoting user awareness, organizations can enjoy the benefits of AR and VR while mitigating potential risks.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- AR/VR: Privacy and Autonomy Considerations – Review this article for an overview of the report issued by the Future of Privacy Forum (FPF) outlining recommendations for tackling privacy risks associated with these technologies.

- Security and Privacy Risks of VR and AR – Discussion of augmented reality security and privacy issues from the security folks at Kaspersky Labs.

© 2023 The vCISO. All rights reserved

9. Biometric Authentication

Topic Description:

Biometric authentication is a method of verifying a person's identity based on their unique physical or behavioral characteristics. It leverages distinct attributes that are specific to an individual, such as fingerprints, facial features, iris patterns, voice patterns, or even behavioral traits like typing rhythm or gait. The process typically involves capturing biometric data using specialized sensors or devices, such as fingerprint scanners, cameras, or microphones. This data is then analyzed and compared against pre-registered templates or reference data stored in a secure database. If the captured biometric data matches the stored template within an acceptable threshold of similarity, the individual is granted access or authentication.

Biometric authentication offers several advantages over traditional methods like passwords or PINs. Firstly, biometric traits are inherently unique to each individual, making it difficult to forge or replicate. Secondly, it eliminates the need for users to remember complex passwords, reducing the risk of security breaches due to weak or stolen credentials. Additionally, it provides a more convenient and user-friendly authentication experience.

However, biometric authentication is not without its challenges. Certain biometric traits may have limitations in terms of accuracy, reliability, or susceptibility to spoofing. For example, a voice recognition system may mistakenly fail to accurately validate a legitimate individual who has laryngitis or a cold. Likewise, such a system may find it difficult to distinguish between the voice of a person and her twin sister. Other concerns regarding the use of biometrics relate to privacy and the secure storage of biometric data. If the stored biometric templates are compromised, they cannot be changed like a password, potentially leading to irreversible security risks. Organizations may want to advocate for policies that prevent storage of original biometric baselines (e.g., images of a face, fingerprint, retina etc.) but allow for retention of a numeric value/calculation derived from those biometrics instead.

Despite these challenges, biometric authentication is widely adopted in various applications, including smartphones, access control systems, financial transactions, and border control. Ongoing advancements in technology and the integration of robust security measures aim to enhance the accuracy, reliability, and overall security of biometric authentication systems.

Policy Discussion:

For the most part, discussions about security and privacy concerns related to an organization's use of biometrics relate to the need to protect the confidentiality and integrity of biometric data. Organizations should therefore expand policies related to the storage and/or encryption of sensitive data to ensure coverage of biometric data as well. To the degree that organizations have not already done so, it will also be necessary to establish policies that outline the collection, use, and storage of biometric data with explicit user consent. Accordingly, organizations need to ensure compliance with relevant privacy laws and regulations, and clearly communicate the purpose, retention period, and rights of individuals regarding their biometric data. And lastly, organizations considering the use of biometrics must develop policies for the authentication and authorization of individuals accessing systems or services using biometric authentication. This includes

© 2023 The vCISO. All rights reserved

defining the process for identity verification, access control mechanisms, and protocols for secure biometric data transmission.

Guidance:
Considerations for using biometric authentication:

- **Biometric Data Protection** – Biometric authentication relies on capturing and storing individuals' unique physical or behavioral characteristics, such as fingerprints, iris patterns, or facial features. Protecting the privacy and security of biometric data is crucial. Encryption, secure storage, and transmission protocols should be implemented to prevent unauthorized access or misuse of this sensitive information.

- **Spoofing & Presentation Attacks** – Biometric systems can be susceptible to spoofing or presentation attacks, where attackers attempt to deceive the system by using artificial replicas or manipulated biometric traits. Robust anti-spoofing techniques, such as liveness detection and behavioral analysis, should be employed to detect and prevent such attacks.

- **Biometric Template Storage** – Biometric authentication systems often store biometric templates, which are mathematical representations of an individual's biometric data. It is crucial to protect these templates from unauthorized access. Hashing, encryption, or tokenization techniques can be employed to secure the storage of biometric templates and prevent reverse engineering or reconstruction of the original biometric data.

- **Centralized Databases & Privacy Concerns** – In some cases, biometric authentication systems rely on centralized databases that store users' biometric data. These databases become attractive targets for attackers aiming to steal or manipulate biometric information. Strong access controls, encryption, and adherence to privacy regulations are essential to protect centralized biometric databases and address privacy concerns.

- **User Acceptance & Perception** – The adoption of biometric authentication may raise concerns among users about privacy, data security, and the potential misuse of their biometric information. Organizations should communicate transparently about the collection, usage, and protection of biometric data. Clear policies, informed consent, and user education can help build trust and foster user acceptance of biometric authentication.

Considerations against using biometric authentication:

- **Irrevocability** – Unlike passwords or PINs, biometric traits are not easily revocable if compromised. If an individual's biometric data is compromised, it cannot be changed like a password. In the event of a biometric data breach, organizations must have appropriate response plans in place to mitigate the potential impact.

- **False Acceptance & False Rejection Rates** – Biometric authentication systems are not perfect and can produce false acceptance or false rejection errors. False acceptance occurs when an unauthorized

© 2023 The vCISO. All rights reserved

person is incorrectly granted access, whereas false rejection happens when a legitimate user is denied access. Organizations need to evaluate the error rates of their chosen biometric system and implement appropriate thresholds to balance security and usability.

- **Single-Factor Authentication** – Biometric authentication, when used alone, constitutes a single factor of authentication. It is recommended to consider multi-factor authentication (MFA) by combining biometric authentication with other factors, such as passwords or tokens. MFA provides an additional layer of security, reducing reliance on a single authentication method.

- **Biometric Data Compromise** – In the event of a successful attack or data breach, compromised biometric data may have long-term implications for individuals. Unlike passwords, biometric traits cannot be easily changed. Organizations must implement robust security measures to prevent unauthorized access to biometric data and have incident response plans in place to mitigate the impact of a breach.

In summary, although biometric authentication offers advantages in terms of convenience and security, organizations should carefully consider and address the cybersecurity considerations associated with its use. Robust data protection measures, anti-spoofing techniques, secure storage practices, user education, and adherence to privacy regulations are essential for the secure implementation of biometric authentication systems.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- Ethics in Biometrics: What Every Security Management Professional Should Know – This article provides an overview of the ethical guidelines crafted by the biometrics community for the responsible use of the various products and technologies they have been developing, producing, and implementing.

- Security and Privacy Requirement for Authentication using Biometrics on Mobile Devices (ISO/IEC 27553-1:2022(en)) – This document provides high-level security and privacy requirements and recommendations for authentication using biometrics on mobile devices, including security and privacy requirements and recommendations for functional components and for communication.

- Biometric Specification for Personal Identity Verification (SP 800-76-2) – This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It describes technical acquisition and formatting specifications for the PIV system, including the PIV Card itself. It also establishes minimum accuracy specifications for deployed biometric authentication processes.

- Using Mobile Device Biometrics for Authenticating First Responders NISTIR 8334 – This report examines how first responders could use mobile device biometrics in authentication and what the unsolved challenges are. This report was developed in joint partnership between the National

© 2023 The vCISO. All rights reserved

Cybersecurity Center of Excellence (NCCoE) and the Public Safety Communications Research (PSCR) Division at NIST.

© 2023 The vCISO. All rights reserved

10.Autonomous Vehicles

Topic Description:

Autonomous vehicles, also known as self-driving cars or driverless cars, are vehicles that can navigate and operate without direct human intervention. They leverage a combination of advanced technologies, including sensors, artificial intelligence (AI), and sophisticated algorithms, to perceive their surroundings, make decisions, and control their movements.

Autonomous vehicles rely on a variety of sensors, such as cameras, lidar (light detection and ranging), radar, and GPS, to gather real-time data about their environment. This information is processed by onboard computers and AI systems, which analyze and interpret the data to understand the vehicle's surroundings, identify obstacles, detect traffic signals, and make informed decisions regarding acceleration, braking, and steering.

The autonomous driving system uses complex algorithms and machine learning techniques to continuously adapt and respond to changing road conditions, traffic patterns, and potential hazards. The goal is to provide a safe and efficient driving experience, minimizing the risk of accidents and improving overall transportation efficiency.

Autonomous vehicles have the potential to revolutionize transportation by offering several benefits. They can enhance road safety by reducing the occurrence of human errors, which are a leading cause of accidents. They also have the potential to increase traffic efficiency and reduce congestion by optimizing routes and maintaining consistent speeds. Additionally, autonomous vehicles can provide mobility options for individuals who are unable to drive, such as the elderly or people with disabilities.

However, the widespread adoption of autonomous vehicles faces various challenges. Ensuring the safety and reliability of autonomous systems is a critical concern, as any software or hardware failure could have severe consequences. Regulatory and legal frameworks need to be developed to address liability issues and establish guidelines for autonomous vehicle operation. Additionally, public acceptance, infrastructure readiness, and integration with existing transportation systems are important factors to consider. Likewise, it is important to ensure that these systems are secure and protected from cyberattacks, as a compromised autonomous vehicle could pose a significant risk to public safety.

Despite these challenges, significant progress has been made in the development and testing of autonomous vehicles by various technology companies and automotive manufacturers. While fully autonomous vehicles are not yet widely available for public use, prototypes and pilot programs are underway, and the future holds the promise of a transportation revolution driven by autonomous technology.

Policy Discussion:

The risks associated with self-driving vehicles are primarily of concern to organizations who provide or require their personnel to use such machines as part of company sponsored activities. The internal communication

© 2023 The vCISO. All rights reserved

systems and external networks upon which such vehicles depend are susceptible to attack which can lead to disruptions in vehicle functionality, compromise of data, and potentially to occupant injury.

- Interconnection risks
- Firmware and software vulnerabilities
- Sensor Manipulation
- Data Privacy and Identity Theft
- Supply Chain Security
- Human-Machine Interaction.

An exhaustive discussion of the means by which the foregoing issues might be resolved is beyond the scope of this document. However, in the vast majority of cases, the risks can be effectively managed by prudent application of existing cybersecurity controls and technologies such as those listed below:

- Encryption
- Authentication Mechanisms
- IDS/IPS
- Testing
- Vulnerability and Patch Management
- Secure Coding
- Resiliency and Redundancy

Guidance:
Considerations for using autonomous vehicles:

- **Secure Communication** – Autonomous vehicles rely on various communication channels, such as wireless networks and vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication, to exchange data and make real-time decisions. Ensuring the security of these communication channels, including encryption, authentication, and integrity verification, is crucial to prevent unauthorized access, tampering, or interference.

- **Protection Against Remote Attacks** – Autonomous vehicles are vulnerable to remote attacks from malicious actors who attempt to gain control of the vehicle's systems. Implementing strong security measures, such as secure boot processes, intrusion detection systems, and robust access controls, can help protect against unauthorized access and manipulation.

- **Software & System Integrity** – The complex software systems and algorithms that drive autonomous vehicles are prone to vulnerabilities. Regular software updates, secure coding practices, and thorough testing are essential to maintain the integrity of the software and mitigate the risk of exploitation by attackers.

- **Sensor Security** – Autonomous vehicles heavily rely on sensors, such as cameras, LiDAR, and radar, to perceive their surroundings. Manipulation or compromise of these sensors can lead to false data input and potentially dangerous situations. Implementing sensor redundancy, tamper-resistant hardware, and integrity checks can help ensure the reliability and security of sensor data.

© 2023 The vCISO. All rights reserved

- **Privacy Of User Data** – Autonomous vehicles collect and process a significant amount of user data, such as location information, driving patterns, and personal preferences. Protecting the privacy of this data is crucial. Implementing privacy-enhancing technologies, anonymization techniques, and secure data handling practices can help safeguard user privacy.

Considerations against using autonomous vehicles:

- **Complexity & Vulnerabilities** – Autonomous vehicles are highly complex systems that incorporate multiple components, software, and communication interfaces. This complexity introduces a larger attack surface and potential vulnerabilities. Thorough security assessments, penetration testing, and continuous monitoring are necessary to identify and address vulnerabilities throughout the lifecycle of autonomous vehicles.

- **Insider Threats** – Autonomous vehicles involve collaboration between various stakeholders, including manufacturers, suppliers, and service providers. Insider threats, such as employees with unauthorized access or malicious intent, can pose significant risks. Implementing strict access controls, separation of duties, and ongoing monitoring can help mitigate insider threats and unauthorized actions.

- **Legal & Liability Concerns** – The deployment of autonomous vehicles raises legal and liability considerations. In the event of accidents or security incidents, determining responsibility and liability can be complex. Clear regulations, insurance policies, and legal frameworks need to be in place to address these concerns and ensure appropriate accountability.

- **Public Trust & Perception** – Widespread adoption of autonomous vehicles relies on public trust and confidence in their safety and security. High-profile incidents or security breaches can erode public trust in autonomous vehicle technology. Transparent communication, comprehensive safety testing, and effective incident response strategies are crucial to maintaining public confidence.

- **Transition & Legacy Systems** – The transition from traditional vehicles to autonomous vehicles may involve integrating new technologies with legacy systems and infrastructure. Compatibility issues, security gaps in legacy systems, and the need for secure over-the-air updates pose additional challenges. Comprehensive risk assessments, secure integration practices, and robust transition plans are necessary to address these complexities.

In summary, although autonomous vehicles offer significant potential benefits, organizations and policymakers must address the cybersecurity considerations associated with their use. Implementing robust security measures, including secure communication, software integrity, and privacy protection, is crucial to ensure the safety and security of autonomous vehicles and gain public trust in this transformative technology.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

© 2023 The vCISO. All rights reserved

- Hackers Remotely Kill a Jeep on a Highway -- Two hackers have developed a tool that can hijack a Jeep over the internet. WIRED senior writer Andy Greenberg takes the SUV for a spin on the highway while hackers attack it from miles away.

- Automotive Hacking: Remotely Hacking Into A Brand-New Car – Watch how Upstream's security researcher hacks into a new car, gains full access into its capabilities, and takes control over the vehicle while being miles away in his office.

- Advanced Cars May Face Greater Risk of Hacking, Cybersecurity Experts Warn – Read this Forbes article to learn how experts at recent auto technology conferences as well as several industry reports paint disturbing pictures of how a severe shortage of skilled software engineers, inadequate planning and testing by automakers before vehicles go into production, unintended entry points such as Bluetooth links and a lack of software standards are all contributing to creating fertile, rolling targets for malevolent hackers.

- The Risk of Automotive Hacking – This article discusses how the rise of automotive hacking is in full force, with many advanced vehicles discovering wireless and other cyber vulnerabilities. This area is becoming a new frontier for car hackers to exploit and learn from.

- Cybersecurity in Automotive: Mastering the Challenge – This article from McKinsey & Company addresses concerns about the increased likelihood of automotive hacking related to the software content of cars.

© 2023 The vCISO. All rights reserved

11. Wearable Technology

Topic Description:

Wearable technology refers to electronic devices or accessories that can be worn on the body, typically in the form of clothing, accessories, or smart devices. These devices are designed to incorporate advanced technologies and sensors to collect, monitor, and transmit data, while providing convenient and seamless integration into the user's daily life.

Wearable technology encompasses a wide range of devices, including smartwatches, fitness trackers, smart glasses, smart clothing, and even implantable devices. These devices are often connected to smartphones or other mobile devices via wireless technologies such as Bluetooth or Wi-Fi, allowing them to interact with other devices or applications.

The primary purpose of wearable technology is to enhance the user's experience by providing real-time information, tracking various aspects of their health and fitness, offering communication and notification features, and even assisting in specific tasks or activities. For example, smartwatches can display notifications, track physical activity, monitor heart rate, and provide GPS navigation, while fitness trackers focus on monitoring steps taken, calories burned, sleep patterns, and more.

Wearable technology has also found applications beyond personal health and fitness. It is being used in industries like healthcare, where devices can monitor patients' vital signs and transmit data to healthcare providers. In the fashion industry, smart clothing can incorporate sensors for activity tracking or environmental monitoring. Additionally, augmented reality (AR) and virtual reality (VR) headsets are considered wearable technology, enabling immersive experiences and applications in gaming, education, and training.

Overall, wearable technology represents a rapidly growing field with the potential to revolutionize how we interact with technology, monitor our health, and augment our daily lives with smart, connected devices. However, as is the case with all technological advancements, it is important to ensure that these devices (along with the data they collect and transmit) are secure and protected from cyber threats.

Policy Discussion:

To a certain extent wearables are no different than any other class of technology asset capable of collecting, storing, processing, and transmitting information. The question then is around whether and under what circumstances said devices may be used and how to control the associated risks.

To begin, wearables collect and transmit a substantial amount of personal data, including health data that owing to limitations of regulations may not be covered by HIPAA despite the fact that the data is of the same sensitivity. If this data is not properly protected, it could be compromised, exposing the organization to liability.

Such devices, although quite capable in some respects, are often far more vulnerable than their traditional IT cousins and may represent an attack surface from which to pivot to interconnected data environments (i.e., both direct domain connections as well as indirect connections through mobile devices). Great care must

© 2023 The vCISO. All rights reserved

therefore be taken with respect to insecure communication protocols (e.g., Bluetooth) and configuration to avert malware, phishing, and social engineering.

Guidance:
As with all technology, wearables must be subject to other security policies:

- Update firmware and apply security patches.
- Govern access control with strong / traceable credentials (passwords and/or PINs)
- Affirmatively evaluate and grant permissions to these devices
- Regularly review and adjust privacy settings.
- Only install applications from trusted/vetted sources
- Avoid connections to insecure/public Wi-Fi.

In summary, wearables offer great convenience and functionality, but organizations must be mindful not to accept risks by default because they lack awareness of their existence.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- 61M Fitbit, Apple Users Had Data Exposed in Wearable Device Data Breach – An independent cybersecurity researcher discovered a wearable device data breach that exposed the records of 61 million Apple and Fitbit users.
- Security Guidance for First Responder Mobile and Wearable Devices (NISTIR 8235) – Guidance from NIST designed to enable jurisdictions to select and purchase secure devices and assist industry to design and build secure devices tailored to the needs of first responders. This guidance can be extrapolated to other use cases as well.
- Cybersecurity Guidance for Connected Wearable Devices – IEEE guidance originally published at the 2022 International Conference on Business Analytics for Technology and Security (ICBATS)

© 2023 The vCISO. All rights reserved

12. Drones

Topic Description:

Drone technology refers to unmanned aerial vehicles (UAVs) or remotely piloted aircraft systems (RPAS) that are equipped with various sensors, cameras, and navigation systems. Drones are designed to fly autonomously or be controlled remotely by operators on the ground. They have gained significant popularity and found diverse applications across numerous industries.

Drones come in various sizes, ranging from small handheld models to larger aircraft capable of carrying substantial payloads. They are typically equipped with multiple rotors or wings that enable vertical takeoff and landing, as well as stable flight control.

One of the key features of drone technology is their ability to capture aerial imagery and videos, providing a unique perspective from above. This capability has revolutionized fields such as aerial photography, filmmaking, and surveillance, allowing for breathtaking visuals and enhanced situational awareness.

Drones have also become an essential tool in industries like agriculture, where they can be used to monitor crops, assess plant health, and optimize irrigation and fertilization processes. In the construction and infrastructure sectors, drones are utilized for site surveys, 3D mapping, and monitoring construction progress. Moreover, drones have shown immense potential in search and rescue operations, disaster management, and environmental monitoring. Their agility, mobility, and ability to access remote or hazardous areas make them invaluable for tasks such as search missions, delivering supplies, or assessing damage in emergency situations.

In recent years, the development of advanced drone technologies has focused on improving flight duration, range, and payload capacity. Additionally, artificial intelligence and machine learning techniques are being incorporated to enhance autonomous flight, obstacle avoidance, and object recognition capabilities.

Although drone technology offers significant benefits, there are also concerns regarding privacy, safety, and regulation. Many countries have implemented specific guidelines and regulations to ensure responsible and safe drone operation. Overall, drone technology has opened up new possibilities in various sectors, providing cost-effective, efficient, and innovative solutions for tasks that were previously challenging or inaccessible.

Policy Discussion:

Drones bring with them great promise and potential benefits. However, their adoption also carries some familiar concerns and introduces new cybersecurity considerations. Thus, as is the case with many other new technologies, the primary policy question is whether and under what conditions organizations choose to allow such devices to be used. Let's explore the cybersecurity considerations for and against using drones:

Guidance:

Considerations for using drones:

- **Secure Communication** – Drones rely on wireless communication links to transmit commands and receive data. Ensuring the security of these communication channels is crucial to prevent

© 2023 The vCISO. All rights reserved

unauthorized access, interception, or hijacking of the drone's control signals or data transmission. Implementing encryption, authentication, and integrity verification mechanisms can help protect against these risks.

- **Unauthorized Access & Hijacking** – Drones can be susceptible to unauthorized access and hijacking by malicious actors. Weak or default passwords, unencrypted control signals, or vulnerabilities in the drone's software or firmware can allow attackers to take control of the drone remotely. Implementing strong authentication, secure configurations, and regular software updates are essential to mitigate these risks.

- **Data Privacy** – Drones may capture and transmit sensitive data, such as images, videos, or sensor readings. Protecting the privacy of this data is crucial, especially when conducting surveillance or data collection activities. Implementing encryption, secure data storage, and adhering to privacy regulations can help safeguard the privacy of individuals and organizations involved.

- **Physical Security** – Physical security of drones is an important consideration. Drones can be physically tampered with, stolen, or damaged, leading to potential risks, including unauthorized access to stored data or misuse of the drone for malicious purposes. Implementing physical security measures, such as anti-tampering mechanisms, GPS-based tracking, and secure storage practices, can help protect against these risks.

Considerations against using drones:

- **Unauthorized Surveillance & Privacy Invasion** – Drones equipped with cameras and sensors can intrude upon privacy by capturing images or recordings without consent. This can lead to concerns related to surveillance and privacy invasion. Implementing strict regulations, obtaining proper permissions, and respecting privacy boundaries are necessary to address these concerns and maintain public trust.

- **Airspace Security & Safety** – Drones operating in shared airspace pose potential risks to aviation and public safety. Unauthorized drone flights or interference with manned aircraft can lead to accidents or disruptions. Implementing geo-fencing, altitude restrictions, and collision avoidance systems can help ensure the safe and responsible use of drones in shared airspace.

- **Infrastructure & System Vulnerabilities** – Drones rely on a combination of hardware, software, and communication systems. These components may have vulnerabilities that can be exploited by attackers. Regular software updates, security testing, and adherence to industry standards can help address vulnerabilities and enhance the overall security of drone systems.

- **Regulatory Compliance** – Operating drones may be subject to specific regulations and restrictions imposed by aviation authorities or local governments. Failure to comply with these regulations can result in legal consequences. It is important for drone operators to understand and adhere to applicable laws, registration requirements, and flight restrictions to avoid legal issues and maintain safety and security.

© 2023 The vCISO. All rights reserved

- **Counter-Drone Threats** – As drone usage expands, so does the potential for malicious actors to employ counter-drone measures to disrupt or intercept drone operations. Organizations need to be aware of potential counter-drone threats and develop strategies to detect, mitigate, and respond to such threats effectively.

In summary, although drones offer numerous benefits, organizations and operators must address the cybersecurity considerations associated with their use. Implementing secure communication, data privacy measures, physical security practices, and adherence to regulations and safety guidelines are crucial to ensure the safe and responsible use of drones while mitigating potential risks.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- Security & Drones: What You Need To Know – Read this Kaspersky Labs article to learn how drones can be hacked and what can be done about it.

- Protecting Against The Threat of Unmanned Aircraft Systems (UAS) -- An Interagency Security Committee Best Practice guide published by DHS/CISA/

© 2023 The vCISO. All rights reserved

13. Smart Homes

Topic Description:

Smart home technology refers to a network of interconnected devices and systems within a house that can be controlled and automated to enhance convenience, comfort, security, and energy efficiency. It involves the integration of various smart devices, sensors, and appliances, which can communicate with each other and be controlled remotely through a central hub or smartphone application.

The core idea behind smart home technology is to enable homeowners to monitor, manage, and interact with their home environment remotely and intelligently. By connecting devices to the internet and utilizing wireless communication protocols such as Wi-Fi or Bluetooth, users can control and automate a wide range of functions.

Smart home devices encompass a diverse range of categories, including smart thermostats, smart lighting, smart locks, security cameras, voice assistants, and home entertainment systems. These devices can be individually controlled or integrated into comprehensive systems that allow for seamless automation and customization.

Through a central control hub or smartphone app, users can remotely adjust thermostat settings, turn lights on or off, lock doors, monitor security cameras, play music, and even control kitchen appliances. Voice assistants like Amazon Echo or Google Home further enhance convenience by allowing users to control their smart home devices using voice commands.

One of the significant advantages of smart home technology is energy efficiency. Smart thermostats can learn and adapt to the homeowners' behavior, optimizing temperature settings and reducing energy consumption. Smart lighting systems can automatically adjust brightness and color based on the time of day or user preferences, saving energy and creating personalized ambiance.

Another important aspect of smart home technology is security. Smart locks provide keyless entry and the ability to remotely grant access to family members or service providers. Security cameras can be monitored from anywhere, and some systems even employ facial recognition or motion detection for added safety.

Although smart home technology offers convenience and improved functionality, privacy and data security are critical considerations. As devices collect and transmit data, it is important to ensure that privacy settings are properly configured and that the devices are regularly updated with security patches.

Overall, smart home technology empowers homeowners to create a more connected and efficient living environment. It provides greater control, convenience, energy savings, and enhanced security through the integration of intelligent devices and systems.

Policy Discussion:

Smart homes, equipped with internet-connected devices and automation technologies, offer convenience and enhanced control over various aspects of a home. However, their adoption also introduces new cybersecurity considerations. Organizations may not be able to dictate what the choices their employees make with respect to the technology they use in their own homes, but companies have an absolute obligation to ensure that company and customer information assets are not inappropriate exposed to impermissible use or disclosure

© 2023 The vCISO. All rights reserved

because of uncontrolled interconnections with insecure home infrastructure. For some organizations it may be a simple matter of expanding upon the guidance already being provided to personnel relative to the configuration of home wireless access points and other smart home technology. In other situations, particularly with respect to highly regulated or sensitive information assets, the organization may find its needs better served by investing in virtualization (i.e., Citrix/VDI) and requiring users who work remotely or from home to rely on company sanctioned solutions instead. Let's explore the cybersecurity considerations for and against using smart homes.

Guidance:
Considerations for using smart homes:

- **Secure Network & Device Connectivity** – Smart homes rely on network connectivity to enable communication between devices. Securing the home network and implementing strong encryption protocols, such as WPA2 or WPA3, is crucial to prevent unauthorized access to smart devices and data transmission.

- **Device Vulnerabilities & Updates** – Smart home devices may have vulnerabilities in their software or firmware, which can be exploited by attackers. Regularly updating and patching smart devices with the latest security updates is essential to address known vulnerabilities and improve device security.

- **Password & Access Management** – Smart home devices often require user accounts and passwords for access. Using strong, unique passwords and enabling two-factor authentication (2FA) adds an extra layer of security. Additionally, managing access privileges for different users and regularly reviewing and revoking access for unused accounts is important to minimize the risk of unauthorized access.

- **Data Privacy** – Smart home devices collect and process a significant amount of personal data, including usage patterns, device statuses, and sometimes audio or video recordings. Protecting the privacy of this data is crucial. Ensuring data encryption, implementing access controls, and carefully reviewing the data handling practices of smart device manufacturers can help protect user privacy.

- **Secure Remote Access** – Many smart home devices provide remote access capabilities, allowing users to control their homes from anywhere. Enabling remote access securely, such as through a virtual private network (VPN) or secure remote access solutions, can help protect against unauthorized access and data interception.

Considerations against using smart homes:

- **Increased Attack Surface** – The interconnected nature of smart homes expands the attack surface, potentially providing more entry points for attackers. Each connected device represents a potential vulnerability that can be exploited. Implementing proper segmentation, firewall rules, and regularly updating all connected devices can help reduce the attack surface and mitigate risks.

© 2023 The vCISO. All rights reserved

- **Dependency On Internet Connectivity** – Smart homes heavily rely on internet connectivity for proper functioning. Loss of internet connectivity can disrupt smart home operations, including security systems, automation, and remote access. Having backup solutions, such as local control options or redundant connectivity, can help maintain essential functions in the event of internet outages.

- **Third-party integrations & vulnerabilities** – Smart home ecosystems often involve integration with third-party services or platforms. The security practices of these third-party providers can vary, and vulnerabilities in their systems can pose risks to the smart home environment. Careful vetting and selection of trusted and reputable third-party integrations is important to minimize these risks.

- **Physical Security Risks** – Smart home devices, such as security cameras or door locks, have a physical presence in the home. These devices can be targets for physical tampering or theft, compromising home security. Implementing physical security measures, such as tamper-resistant hardware, proper device placement, and secure mounting, can help mitigate these risks.

- **User Awareness & Education** – The effective and secure use of smart home devices relies on user awareness and education. Users need to understand the risks associated with smart home technologies, the importance of security practices, and the potential consequences of insecure configurations or actions. Regularly educating and updating users about best practices and emerging threats is essential to maintain a secure smart home environment.

In summary, although smart homes offer convenience and control, it is important to address the cybersecurity considerations associated with their use. Implementing secure network connectivity, regularly updating devices, managing access and passwords, and protecting user privacy are essential practices. It is equally important to be mindful of the expanded attack surface, potential vulnerabilities in third-party integrations, physical security risks, and the need for user awareness and education to ensure a secure smart home environment.

References:
The following resources are intended to illuminate the foregoing academic discussion and help readers think through policy tailoring decisions based on concrete examples:

- Locked Out – Read this account of a customer locked out of his Alexa account by Amazon, rendering all of his smart home devices nonfunctional for a week, because a delivery driver thought his doorbell said something racist.

- How to Protect Your Smart Home From Hackers – Smart homes offer convenience and security risks. Here's what you can do to stop hackers from taking control of your smart speaker, thermostat, doorbell, and other connected devices.

© 2023 The vCISO. All rights reserved