ISSA
Information Systems Security Association

Central Maryland Chapter

Stakeholder Management in Cybersecurity…

April 23rd, 2025

Brian Vaughn, Managing Director

TECHNOLOGY TRANSITION PARADIGM

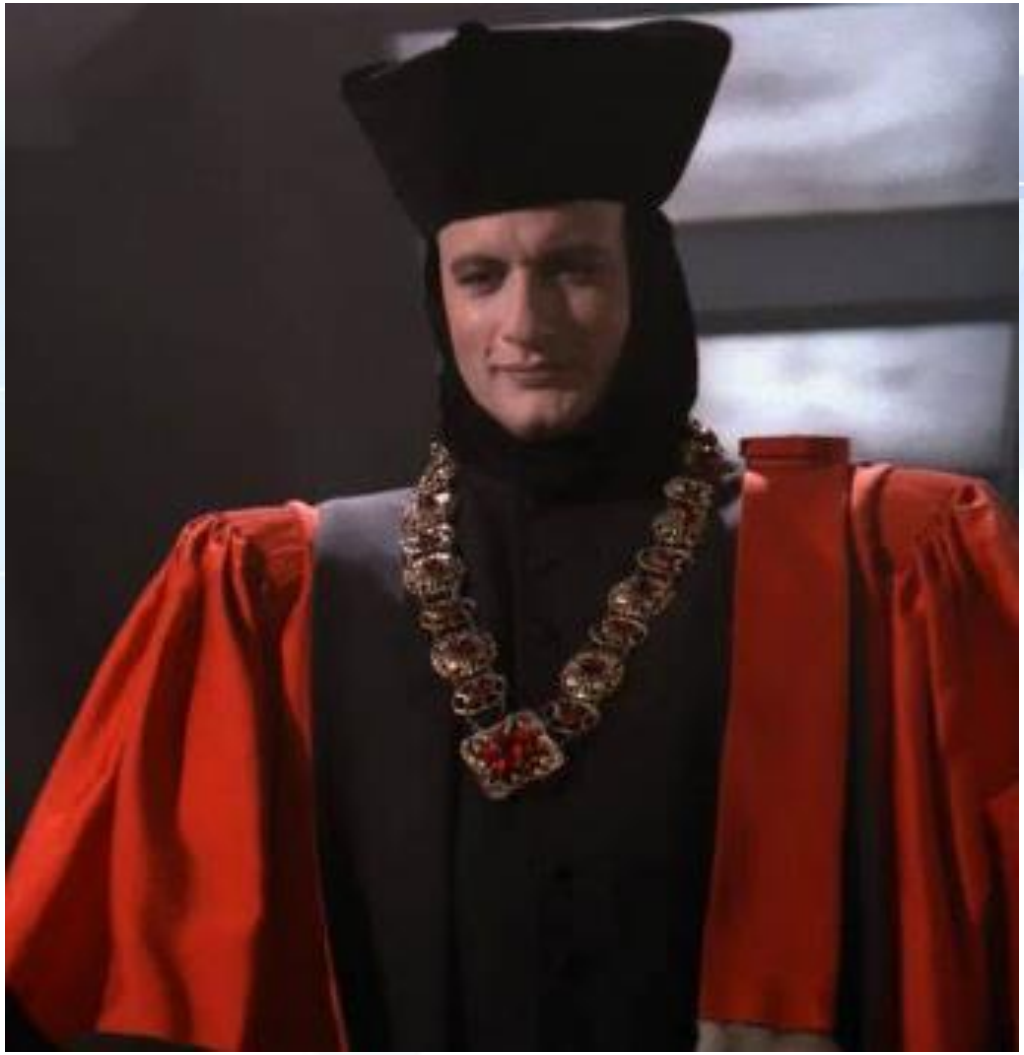
Data Driven | Results Oriented

Stakeholder Management in Information Security…

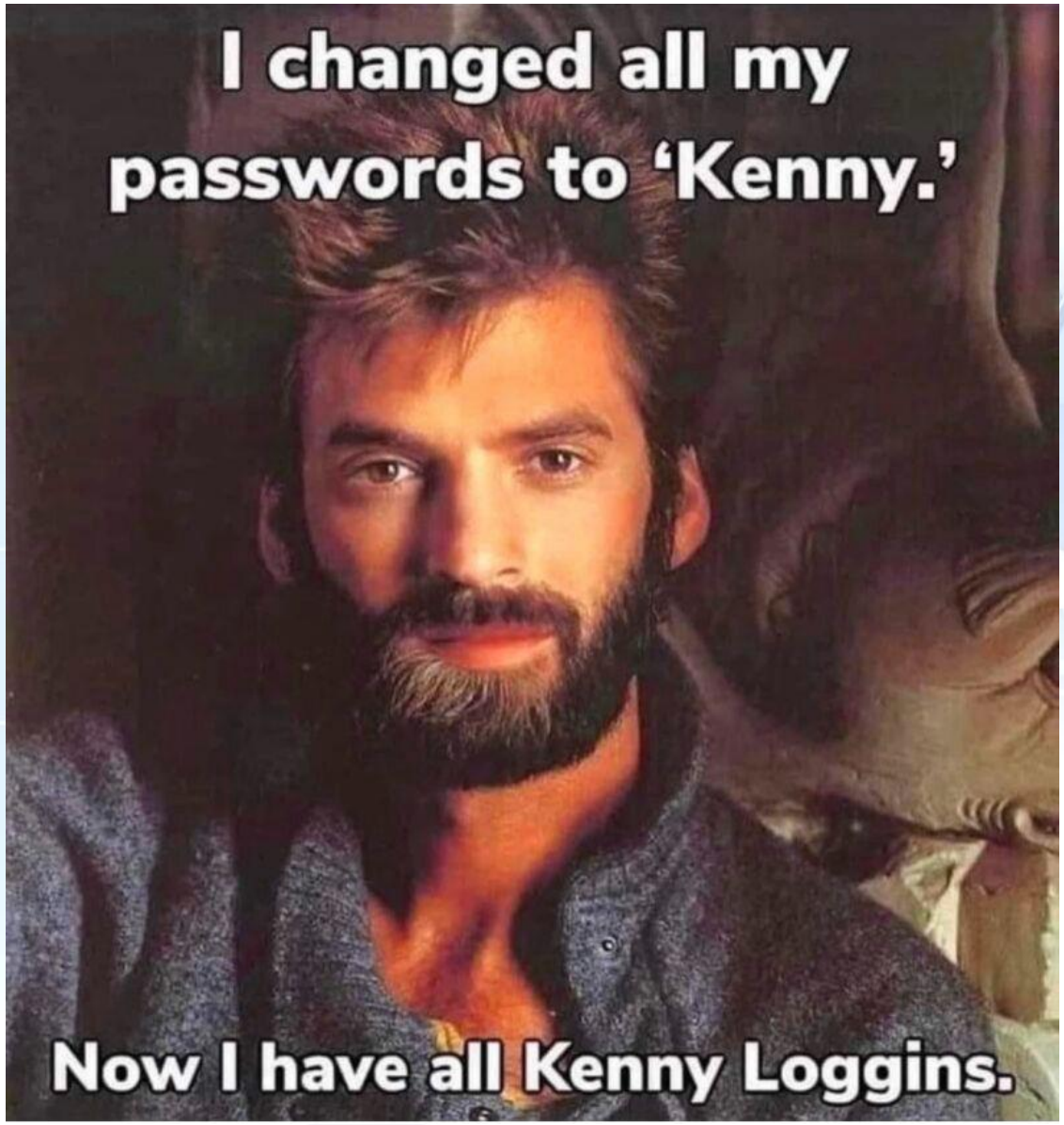
- Supervisor/Manager/Co-Worker
- Client/Customer
- Prospective Client or Manager

If they would just listen to us…

All Knowing & All Powerful



They often will. IF we find their security gaffs, teach how to check and what to do for remedies…


I changed all my passwords to ‘Kenny.’
Now I have all Kenny Loggins.

Stakeholder Kenny Loggin's Gaff Inventory:

- The prospect has recent credential sets (User name & PW) from himself and three dozen of his employees available for sale on a Dark Web ID Theft forum.
- The prospect does not enforce regular password changes on any staff.
- The prospect didn't have three of the four DNS mail handling and authentication security protocols enabled.
- The prospect did not have multifactor authentication on their remote access VPN.
- The CEO's compromised credentials have Global Admin Privileges for Office 365/Azure. His password was only seven digits, and only numeric.
- This was his only account and his user name was his email address. 😲

The ‘Kenny Loggins Lessons’ for business owners, C-level, & Operations management are the following:

- If the IT Department/Supervisor/IT Vendor isn’t advocating basic security Group Policy / Intune Policy for Entra AD such as password strength mandates & password change frequency, it’s a 
- If the IT Dept/Your Boss/Your MSP isn’t asking questions about, nor proposing solutions for Password Vaults, off-line / air-gapped data backups, conditional access, & Internet Security Awareness Training (ISAT), then you have a vendor that is not prioritizing security on your technology roadmap. 
- If Stakeholders lack a formal on-boarding procedure that includes inspecting, & when needed - fixing prior failures of DNS mail handling and authentication security protocols; it demonstrates a lack of pro-active management on important security elements. 
- If the long term IT Department/staff, MSP or consultant has left their client’s remote access VPN in place without configuring it for multi-factor authentication, your vendor is taking you on a Ride Into the Danger Zone. 

Technical Sophistication Level - ??

Dark Web Monitoring: Check If Credentials Are For Sale

Why It's Important:

- The dark web is a marketplace for stolen data.
- Early detection allows immediate action to prevent further damage.

How to Check the Dark Web:

- Contact Transition Paradigm at info@transitionparadigm.com or call 800.889.8072 Ext. 2 for a complimentary dark web monitoring report.
- Use services like Norton for one-time searches or continuous monitoring. Or LastPass. Which is known primarily as a password manager, LastPass also offers dark web monitoring as part of its service, starting at $4.25 per month.
- Prices range from $10 per month to several thousand dollars per month for enterprise solutions.

Why It Matters:

- Knowing if data is on the dark web allows immediate action to safeguard the company's assets.
- Reduces the impact of data breaches and enhances overall security posture.
- Protects against subsequent ‘personal’ disclosures…

Experian:
• Create or log in to your Experian account.
• Select "Add a Security Freeze."
• Provide your personal information
• Verify your identity (this may involve answering security questions or providing documents).
• Once verified, your credit file can be frozen, preventing new credit inquiries.
• You can lift the freeze temporarily or permanently using your PIN or password when needed.

Equifax:
• Create or sign in to your Equifax account.
• Select "Place or Manage a Freeze."
• Enter your personal information for identity verification.
• Confirm your request, and your credit file will be frozen across Equifax.
• To unfreeze, log back in and lift the freeze as desired.

TransUnion:
• Create or log in to your TransUnion account.
• Select "Freeze My Credit" from the dashboard.
• Verify your identity by providing necessary personal information and security verification.
• Confirm your freeze, and your TransUnion credit report will be inaccessible to creditors until you lift the freeze.
• Go to the dashboard to unfreeze your credit as needed.

Major, recent, large-scale data breaches…

1. **AT&T (July 2024)** - Hackers exploited a vulnerability in the third-party cloud platform Snowflake, affecting nearly all of AT&T's wireless customers. The breach exposed call and text metadata, including phone numbers and timestamps 1

2. **New Era Life Insurance Companies (February 2025)** - A cyberattack compromised the data of approximately 335,506 individuals, including names, birth dates, insurance ID numbers, claim information, and social security numbers

3. **Legacy Professionals LLP (February 2025)** - An accounting firm experienced a data leak affecting over 215,000 people. Sensitive identifiable information was accessed following suspicious activity on its computer network.

4. **Hillcrest Convalescent Center, Inc. (March 2025)** - A cyberattack exposed information belonging to 106,194 individuals, including names, dates of birth, social security numbers, patient data, medical information, treatment information, health insurance information, and healthcare provider information

5. **Authority of the City of Bainbridge and Decatur County (February 2025)** - Unauthorized access to desktop computers, laptops, and network servers affected over 120,000 individuals

Enable Microsoft 365’s Free ‘External Email Tagging’

What It Is:

- Microsoft 365 offers an External Email Warning adds an "External" tag to emails received from outside your stakeholder’s organization, helping identify potential phishing or spam emails.
- Displays a notification banner on external emails to alert users.

How to Implement:

- Use the Exchange Online PowerShell command Set-ExternalInOutlook.
- Banner appears on all incoming external emails.

Why It Matters:

- Enhances email security without additional cost.
- Fundamental part of a robust email security strategy.
- Significant oversight if not implemented by the MSP or IT provider.

Best Practices for Managing Global Administrator Rights

Separate Accounts for Different Tasks:

- **Global Admin Account:** Used exclusively for administrative tasks.
- **Daily Driver Account:** Used for regular, day-to-day activities.

Email Address Usage:

- **Daily Driver Account:** Typically associated with the user's email address.
- **Global Admin Account:** Uses an obscure username to enhance security.

Why It Matters:

- **Enhanced Security:** Reduces the risk of hackers gaining full control of the network if credentials are stolen.
- **Minimized Exposure:** Limits the use of Global Admin rights to necessary administrative tasks only.

Air-Gapped Backups: Stakeholder's 'Ransomware Fail-safe'

Offline copies of stakeholder critical data, stored on external media that are not connected to their network or the internet.

Why It's Important:

- Provides an extra layer of security by storing data offline.
- Ensures data can be restored without paying ransom or facing prolonged downtime.

How to Implement:

- Create offline backups using external hard drives, thumb drives, or other removable media.
- Store these backups in a secure, remote location (e.g., different site, safety deposit box, secure storage facility).

Why It Matters:

- Enhances resilience against ransomware that can encrypt or destroy online backups.
- Protects data from physical threats like fire, theft, or natural disasters.

Ensure Proper DNS Configuration

What is DNS and Why is it Important?

- DNS (Domain Name System) translates domain names into IP addresses.
- Acts as the Internet's traffic cop/postal carrier, managing domain addresses for emails and web traffic.
- Examples of DNS Host Providers: GoDaddy, Network Solutions, Cloudflare.
- Ensures mail authentication and handling security protocols to keep mail secure and prevent domain hijacking. DKIM, SPF & DMARC

How to Check the Security Level of Your DNS Setup:

- Use free DNS inspection tools with user-friendly, color-coded interfaces.
- EasyDMARC: Check DNS records at www.easydmarc.com. www.EasyDMARC.com
- MXToolbox: Verify DNS setup at www.mxtoolbox.com. www.MXToolbox.com

Why It Matters:

- Proper DNS security protocols are fundamental yet essential.
- Unresolved security gaps are a significant concern.
- Transition Paradigm can address DNS shortcomings in under an hour.
- Red or Yellow indicators suggest other security measures may be neglected.

Password Vaults

Why It's Important: Password vaults securely store and manage your passwords, ensuring they are strong and unique for each account. This reduces the risk of data breaches caused by weak or reused passwords.

How to Implement:

1. **Choose a Provider:** Some big names include Password Boss, IT Glue, Dashlane, and LastPass.
2. **Cost:** For a 50-person company, recurring costs typically range from $4 to $12 per user, per month. Project/conversion price is typically $1,000 to $3,000

Why It Matters: Facilitating and enabling encrypted password vaults for all users is crucial. Remember, Chrome's password manager is not secure.

Conditional Access

Restrict countries from which staff can log-in

Why It's Important: Restricts system access from high-risk countries like Eastern Europe, Russia, and China.

How to Implement:

- First procure Microsoft 365 'Business Premium'. As of Q1 2025, the price for Business Premium is ~$22 per user per month, vs $15 for Microsoft 365 'Business Standard'. 5% increase for monthly payers on annual plans starting 4/1/25.
- Migrate your legacy Active Directory MS solution to Entra ID and leverage Microsoft Intune.
- Once Intune migration is complete, technical staff can enable conditional access settings in your network security protocols. Which will enable you to restrict log-in access to your corporate network, by country – as you so choose.

Why It Matters: Reduces the risk of unauthorized access from regions known for cybercriminal activity.

Remove “Local Admin Rights” for every standard user.

This is generally achieved using Group Policy in legacy Microsoft/ADDS environments, via Intune in Entra ID environments, or using third-party tools like Auto-Elevate or ThreatLocker.

Why It's Important:
Removing local admin rights for standard users is crucial to minimize security risks, prevent unauthorized changes, and protect sensitive data from potential threats.

How to Implement It:
Group Policy in ADDS: Create a Group Policy Object (GPO) that removes local admin rights and link it to the appropriate Organizational Units (OUs) in Active Directory.

1.Intune: Configure device restriction policies in Microsoft Intune to ensure standard users do not have local admin rights on their devices.

2.Third-Party Tools: Utilize tools like Auto-Elevate or ThreatLocker to manage and enforce application permissions, ensuring users only have the necessary rights for their tasks without local admin privileges.

Security Awareness Training

Why It's Important: Educated employees are your first line of defense against cyber threats, especially email phishing. Understanding cybercriminal tactics helps employees recognize and avoid threats, protecting sensitive information and maintaining system integrity.

What It Includes: Internet Security Awareness Training (ISAT) features:

•Training Videos: Covering essential security topics.

•Phishing Simulations: Testing and reporting employees' ability to identify phishing attempts.

•Compliance Reporting: Tracking training completion and compliance.

Why It Matters: Regular training keeps employees informed about the latest threats and response strategies, ensuring a strong security posture and minimizing the risk of successful cyber attacks.

TECHNOLOGY
TRANSITION PARADIGM
Data Driven | Results Oriented

Brian Vaughn, Technology Transition Paradigm, LLC
bvaughn@TransitionParadigm.com
240.994.5872