Ransomware

A RISK MANAGEMENT STRATEGY

Outline

What is Ransomware?

Impact Analysis

In 2022, **71 percent** of companies worldwide were affected by ransomware.

WORLDWIDE IMPACT

72 percent of the respondents paid the ransom and recovered the compromised data.

HOW MANY PAID THE RANSOM

54 percent of organizations worldwide who regained access to data after first ransom payment

GAINED ACCESS AFTER RANSOM PAYMENT

What Can You Do?

- Get Clear – Risk Analysis
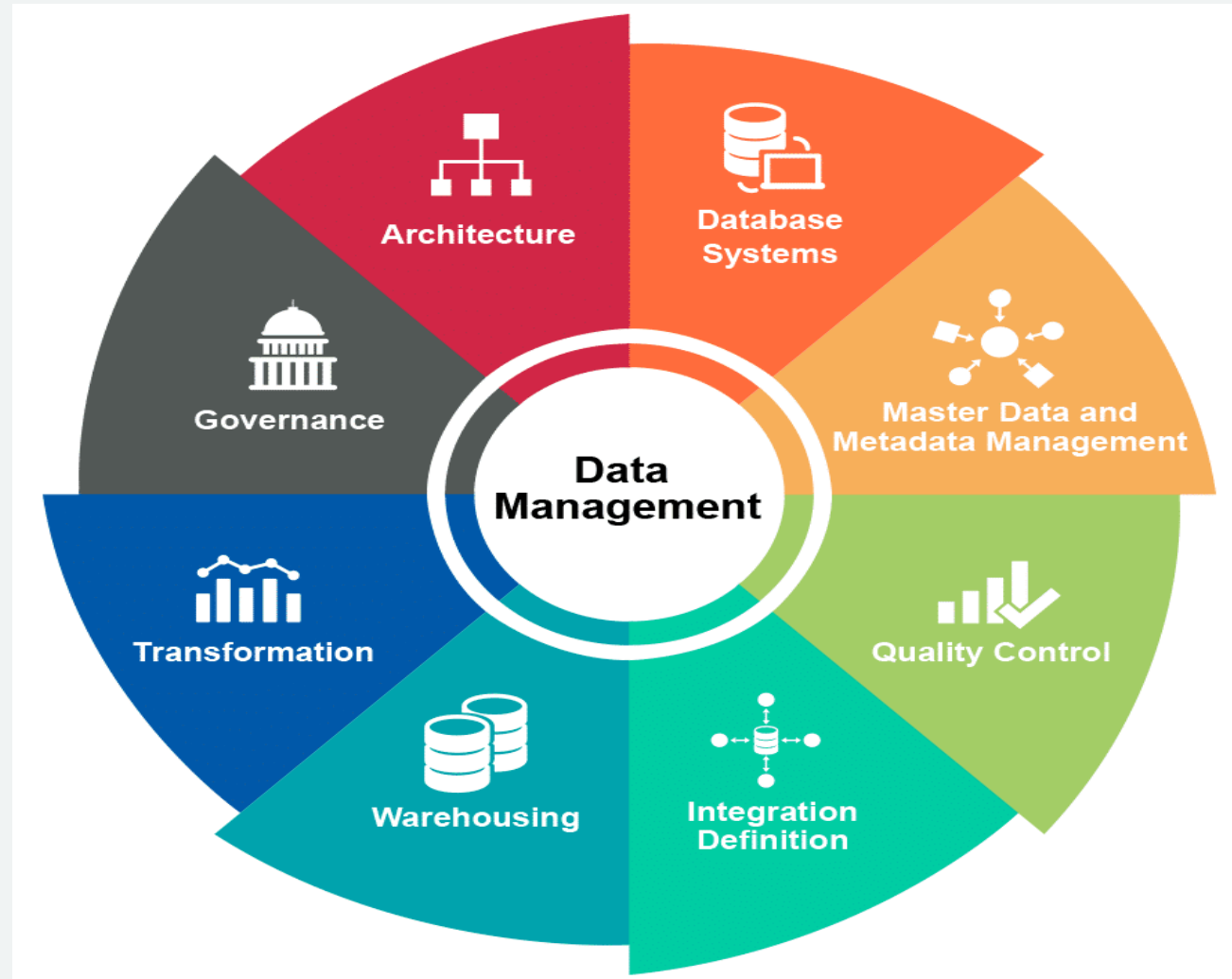
- Mitigation Strategies

Risks Analysis: Get Clear

Risk Assessment – Business & Mission Perspective

- How do you meet client requirements?

- What information is needed to meet these requirements?

- Who should be handling or viewing this information and why?

Risks Analysis: Data Governance Roadmap

Basis of your data governance roadmap to narrow the focus for adequate protection and recovery.

Data Governance Organization Structure (no date) *Blogspot*. Available at: https://jackrowansflightlogs.blogspot.com/2020/11/data-governance-organization-structure.html (Accessed: January 25, 2023).

Mitigations: What is your Strategy?

- Strategy and a Plan for Ransomware Event

- Strategy Plan should cover
    - ❑ Pre - Event
    - ❑ During
    - ❑ Post – Event

- Goal – Return to normal operations as quickly and cost effectively as possible.

Mitigations: Data Backup & Recovery

Do you know exactly what you need to back up? Everything is not the right answer

- Cost of storage

- Categorize and prioritize the data-backups

- Testing of backups

- Securing of backups

- Re-deployment of backup data. It becomes useless if you can't get to what you need, when you need it.

Mitigations: Redundancy

Redundancy of critical systems and processes (Pre)

- Re-routing of critical processes

- Finance/ Accounting

  *Bank accounts

- HR/Payroll

- Client/Site data

- Vendor/Supply-Chain
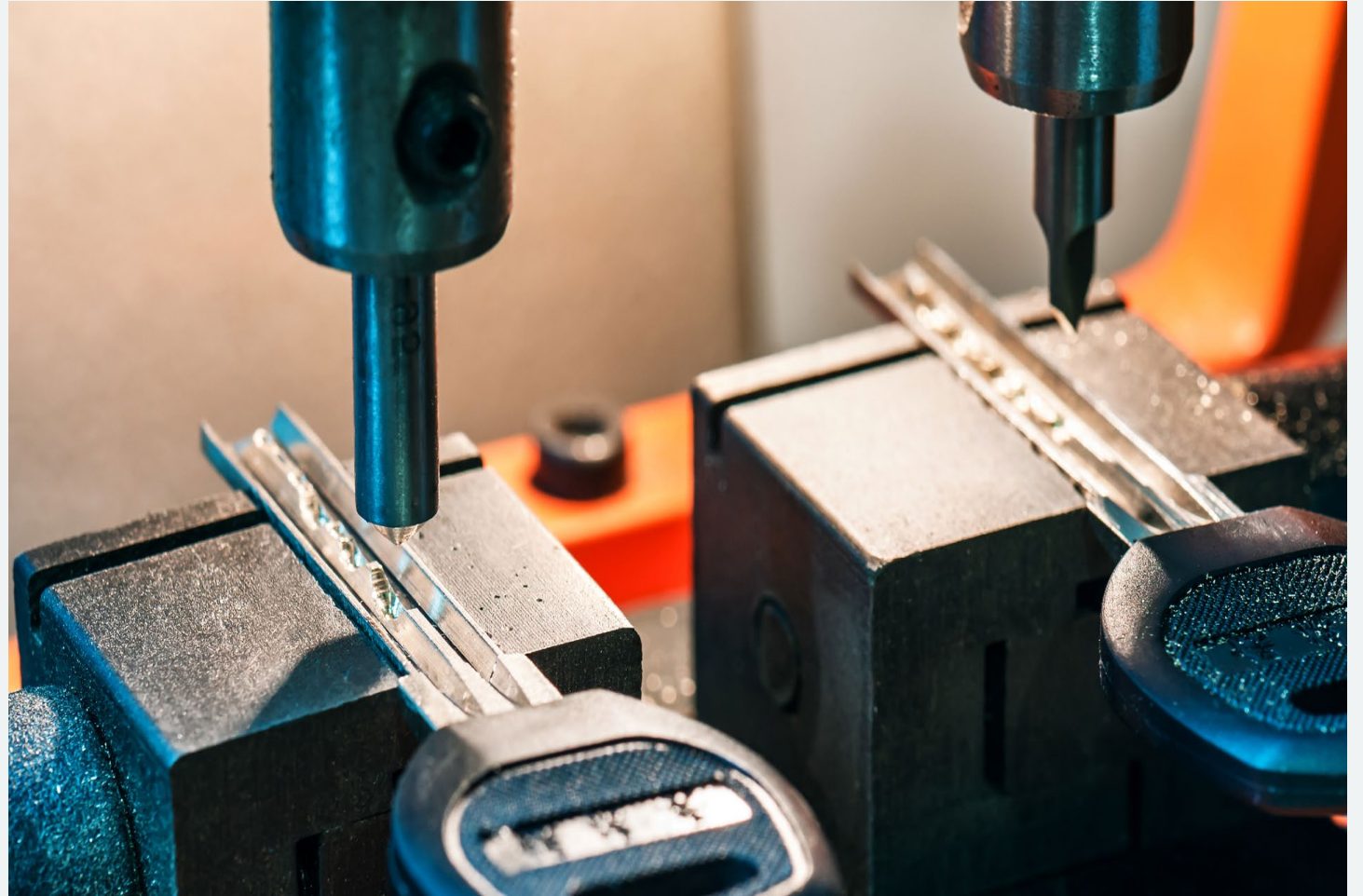
Mitigations: Agreements/ Services & Accounts

Agreements in place:(Pre/During/Post)

- Data breach/privacy call enter support

- Law firms - that specialize in ransomware negotiations

- Forensics support

- Insurance liability coverages

- Crypto-Currency Account established

Mitigations: Communications

Communications Plan (Pre/During/Post)

Call List:

- Law enforcement (FBI, Local Authorities)
- Legal
- IT (Internal/External)
- Data-breach support
- Media Spokesperson

- Name, Numbers, Emails, Alternative contact information

Mitigations: Table-Top Exercises

Table-Top Exercises (Pre/Post)

- Engage all stakeholders

- Jointly discover weaknesses in your responses to mitigate

- Insight on how everyone responds under pressure

- Practice makes perfect

Mitigations: Tools/Resources

Sherwood Applied Business Security Architecture – SABSA
SABSA is a model and methodology for developing a risk-driven enterprise information security architecture and service management, to support critical business processes.
Website: https://sabsa.org/

Data Governance

Cyber Risk Portal - CRP
Use AI to obtain and track cyber risks across your organization to include supply chain and third-party supplier networks in minutes. Includes a free local risk assessment.
Website:
https://www.covenantsec.com/cyber-risk-portal

Risk Assessment

The CyberFish
This platform helps businesses and government teams prepare to better handle business disruptions, by improving effectiveness and resilience of crisis management teams.

Website:
https://www.thecyberfish.com/

Table-Top Exercises

Questions

Judge a man by his questions rather than his answers.

- Voltaire

Keep in touch with us
SIMPLE CYBERSECURITY MANAGEMENT

Website

https://www.covenantsec.com

Locations

United States | Latin America | Africa | India

Contact Info
General Inquiry: info@covenantsec.com
Training: cybersec@covenantsec.com

Telephone

Office Phone: +1 (866) 824 8022

COVENANT
SECURITY SOLUTIONS