Your Lucky Charm: Cyber Insurance Compliance

March 29th, 2024

Tim Lewis & DuRand Bryant

Agenda

- Methodology
- Factors in determining cybersecurity insurance eligibility/premiums
- How industry and business type/size affect cybersecurity insurance and compliance
- How your data sensitivity and volume relate to cybersecurity insurance
- Security measures, policies, and preparation
- Q&A

Introduction

- CyberCrime & Attacks Continue to Rise
- Insurance Providers are getting more particular about their requirements and determining rates
- Our goal is to help navigate the application and remediation process.

Methodology

- The findings in this report were derived from several sources including real-world insurance questionnaires, insurance industry reports and cybersecurity resources
- Insurance statistics were analyzed based on factors such as industry, organization size and history
- Additionally, we attempted to provide information for how insurance requirements are weighted when determining premiums

Key Findings

Things You Cannot (Or Don’t Want To) Change

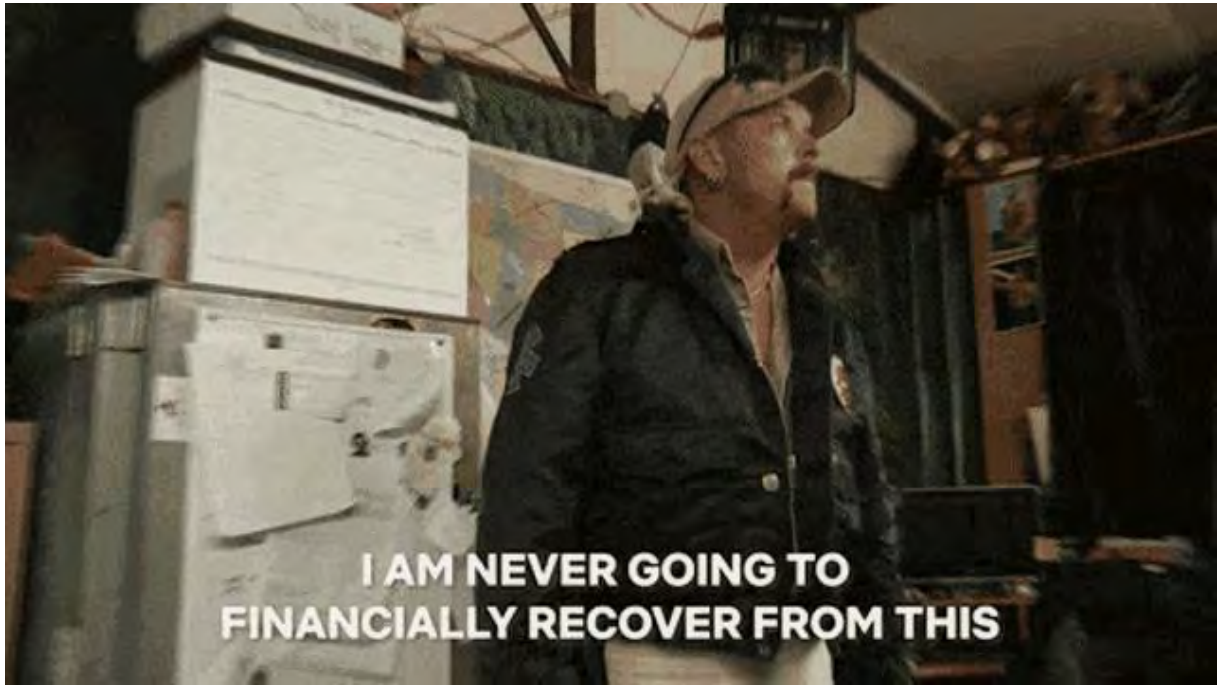
- Industry
- Business Type
- Size & Footprint
- Data Sensitivity

Industry & Business Type (The Highest Risk)

- Healthcare
- Financial Services
- Technology & IT Services
- Retail & e-Commerce
- Energy & Utilities
- Legal & Professional Services
- Education

Size, Financial Health, & Footprint

- The size of the business (revenue, headcount, customers, etc.) present a larger attack surface.
- More revenue means higher ransom (i.e. the bad guys have a DNB account).
- Your ability to financially recover.



Data Sensitivity & Volume

- PII and/or PHI
- Financial Information and/or Payment Card Information
- Authentication Credentials
- Other Sensitive Data Types

Let’s Talk About The Things You CAN Control…

Risk Assessment & Management

- Performing and *documenting* a risk assessment.
- Performing and *documenting* regular pen tests or other security assessments.
- Data Classification.

Employee Security Awareness Training

- SAT is more than a one and done training.
- This is a huge requirement.
- As of 2021, 98% of all cyber-attacks involved some form of social engineering
- Security Awareness Training is universally mentioned in cyber insurance questionnaires

Authentication & Access Controls

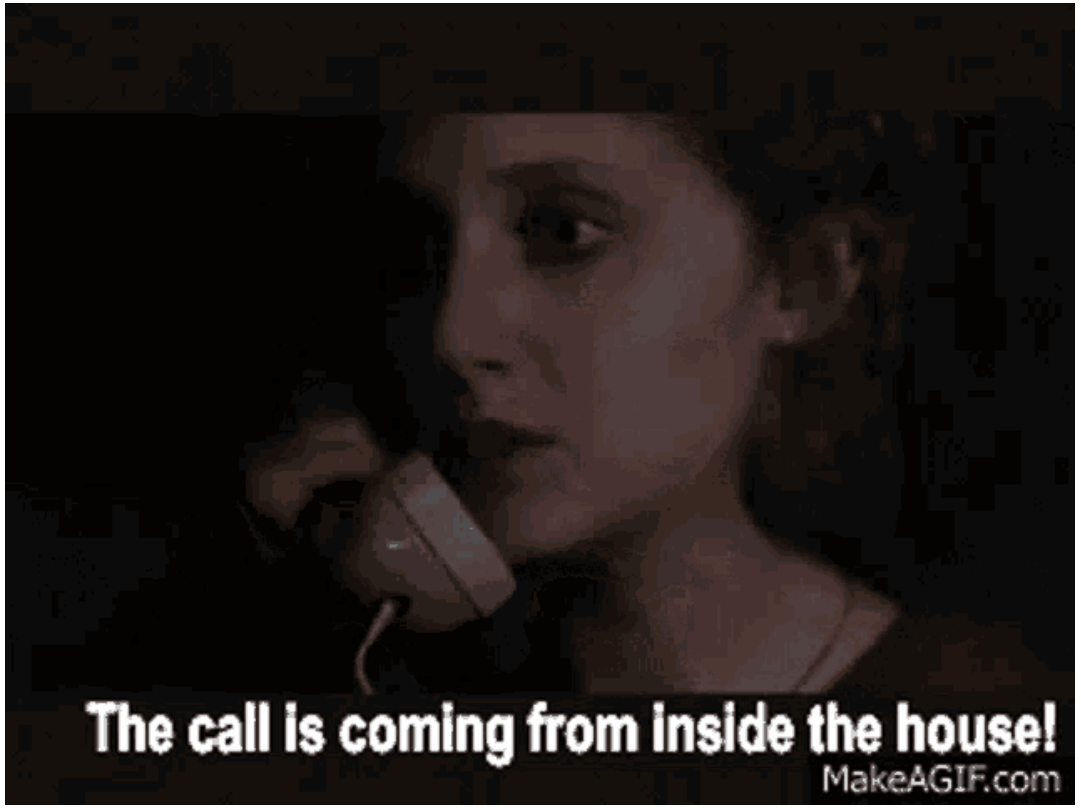
- Implementing strong authentication mechanisms, such as multi-factor authentication , and enforcing strict access controls ensure that only authorized individuals have access to sensitive systems and data
- Adopt a “zero-trust” philosophy for access to systems and data

Endpoint Security

- Endpoint Security is more than just AV.
- Includes a policy for regular AND emergency system patching.
- NOTE: They may want things like “definition updates” and “scheduled scans” though modern endpoint protection has moved beyond this.

Firewalls & Network Security

- Firewalls with anything out/nothing(very little) in no longer fits the bill.
- Insurance companies are now asking for IPS, web filtering and other advanced firewall features.
- Network segmentation and even micro-segmentation is being requested for networks.
- Dedicated IoT and BYOD networks are a plus.



Data Backup & Disaster Recovery

- Have Backups (DUH!)
- Backups should be tested with the results documented.
- Have a documented, reviewed & tested backup & disaster recovery plan.
- Extra steps should be taken to “harden” your backup systems against attack.
- Specifically, MFA is called out.

Patch Management

- For more than your OS’s
- Public facing services like VPN, RMM and others have been targeted.
- Yes, have a plan for patching your switches as well.
- Vulnerability monitoring and management plan.

Security Monitoring & Logging

- Continuous monitoring of network and system activities, along with robust logging practices, enables the timely detection of suspicious behavior
- Security information and event management solutions can assist in aggregating and analyzing log data
- DLP technology should be leveraged as well.

Incident Response Planning & Testing

- A well-documented & tested incident response plan.
- This plan should outline the steps to be taken to contain, eradicate, and recover from a security breach.
- Assessing and managing the cybersecurity practices of third-party vendors.

Encryption

- Encrypting sensitive data, both in transit and at rest.
- This includes encrypting communication channels, databases, and any other storage systems containing sensitive information.
- Endpoint based encryption like Bitlocker or File Vault are included with all operating systems.
- Email encryption policy.

Penetration Testing & Vulnerability Scanning

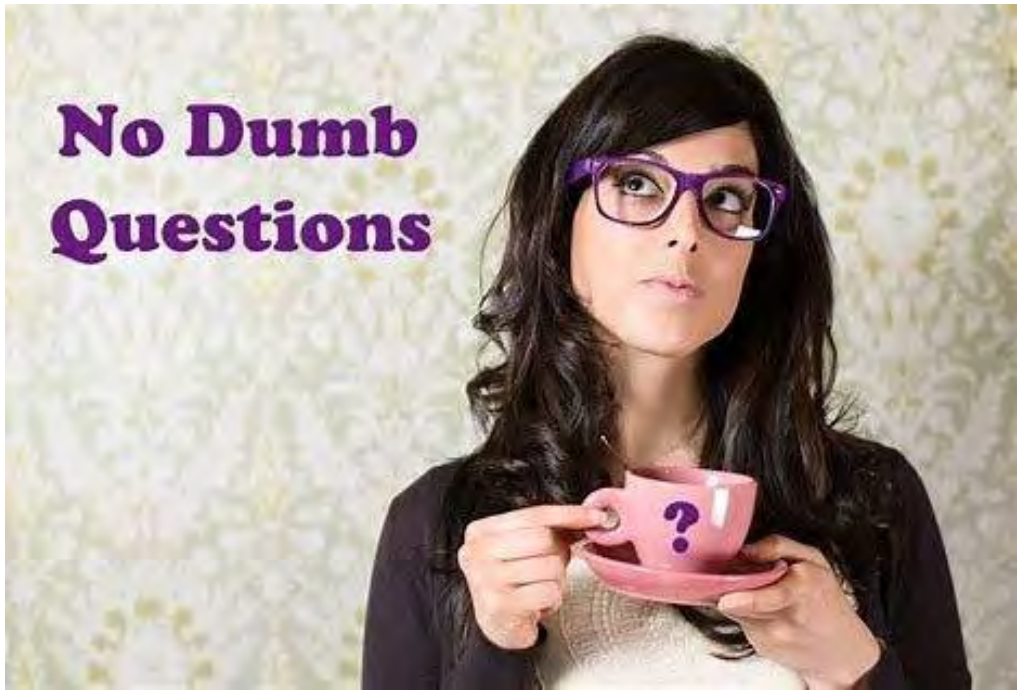
- Regularly testing systems for vulnerabilities through penetration testing and vulnerability scanning helps identify and address potential weaknesses before they can be exploited

History of Cyber Incidents

- If you have had a previous cyber incident or claim, it will dramatically increase your premiums
- The best way to prevent a cyber incident is to execute the things documented here
- Additionally, insurance companies are beginning to require proof of compliance with items outlined in your questionnaire or survey

Some of the Questions We've Seen…

- Some of these are harder to navigate than expected.
- The people writing the questions understand buzzwords, but not the reality of what it means.
- Sometimes "the right answer" is simple, but not easy.
- Documentation & Paperwork is KING for these people.



(SARCASM)

Do You Have Written Procedures For…

- How changes are made to information security components, programs and, yes, written procedures…
- How confidential information is handled, but just on mobile devices.
- Your information security plan
- Hiring/firing employees
- On-boarding contractors
- Business continuity plan

Do You Have MFA…

- For remote access to the network?
- For access to cloud services? *Just cloud services, not that there's many.*
- For remote and local administration… for ALL SYSTEMS.

Compliance, Compliance, Compliance

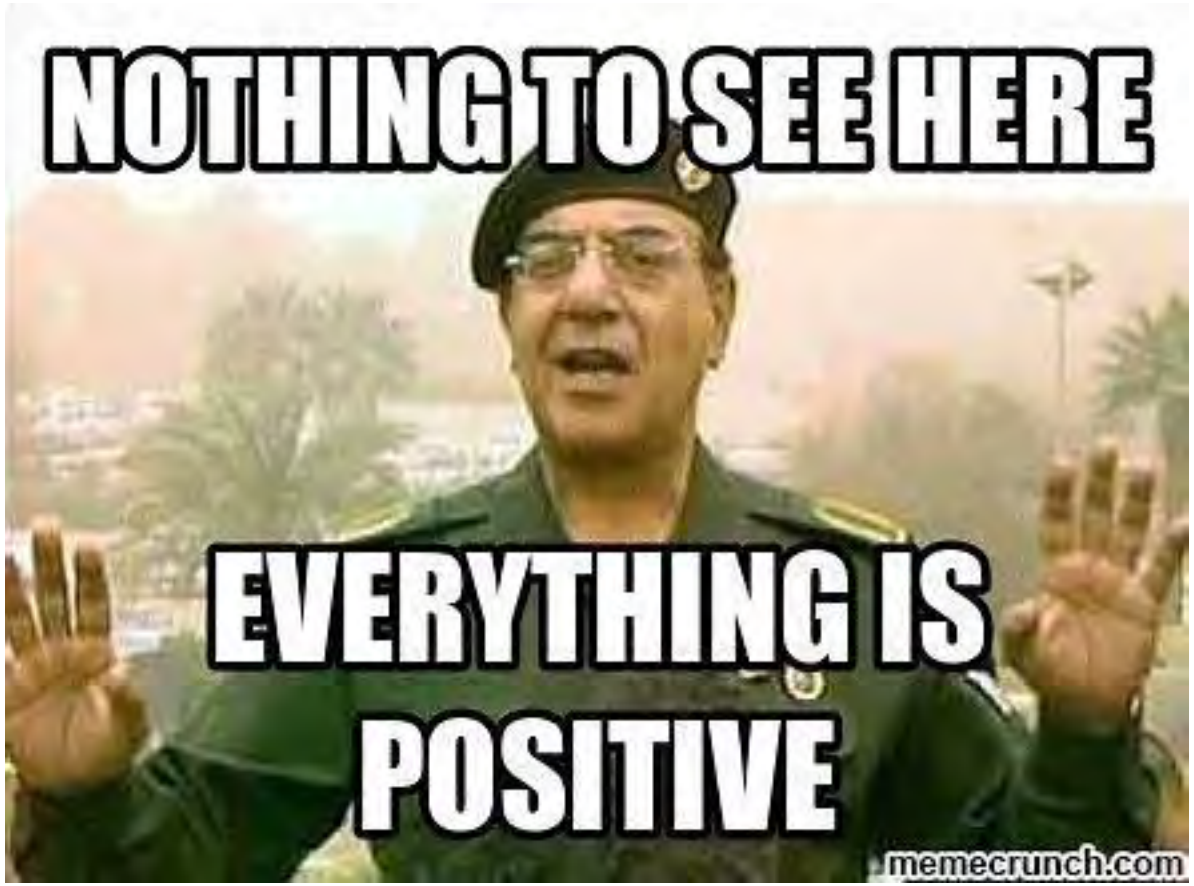
- PCI-DSS (a big one)
- HIPPA (another big one)
- Some have asked about NIST and CMMC compliance

Business Activities

- There is almost always questions about company finances.
- How are you accepting payments and how much for each way?
- Where does your revenue come from?
- They want to know about your clients as well
- How do you handle customer complaints?
- Do you use contracts?
- Do you require customers to sign on project scope changes?

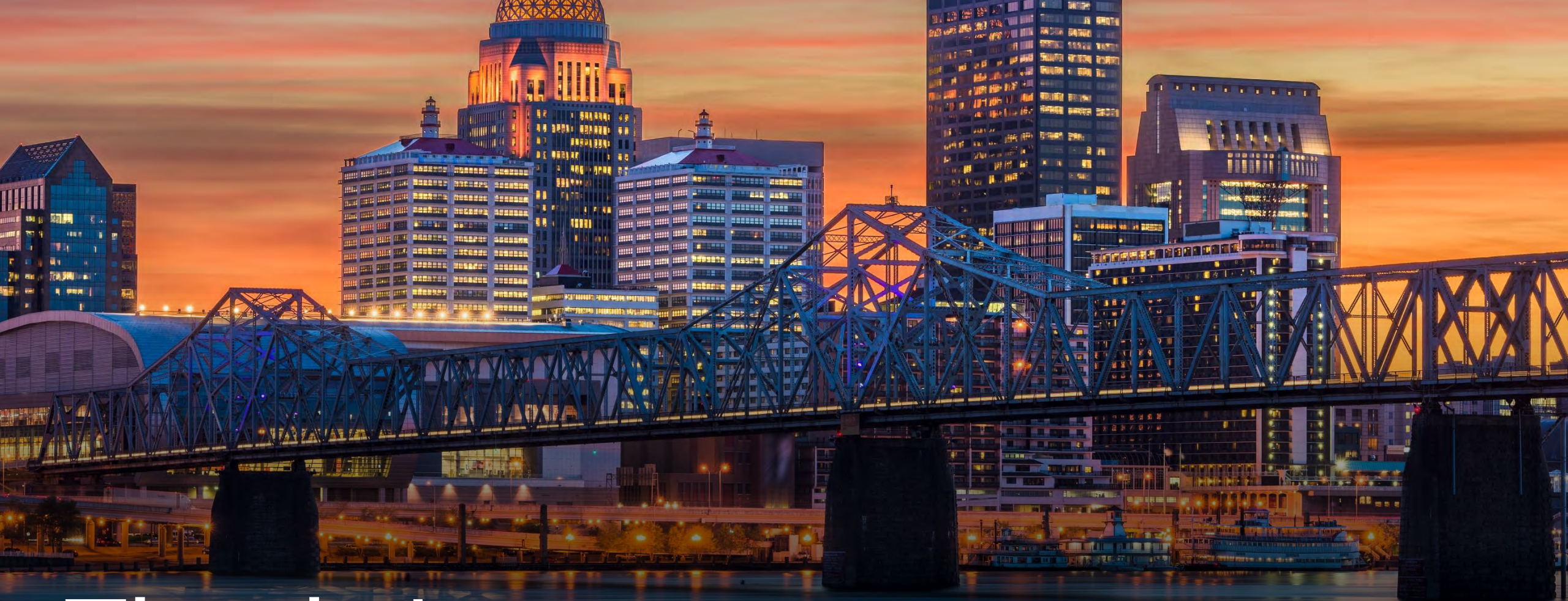
Types of Coverage Include…

- Errors and Omissions
- Legal help.
- Media & Public Relations Help.
- Fraud and Funds Transfer.
- All kinds of wacky things.



Closing / Q&A

- Attaining cyber insurance can be a daunting task
- It is, however, manageable with an organized approach AND meeting the security requirements may help prevent an incident



Thanks!

Tim Lewis
tim.lewis@mirazon.com

DuRand Bryant
durand.bryant@mirazon.com