Cheers to Compliance

Cybersecurity
Hot Topics & IT Exam Focus Areas

Jake Martin
Cybersecurity & IT Resource Specialist
Michigan Department of Insurance and Financial Services
Tel:517-230-5533
MartinJ47@michigan.gov

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Cybersecurity (compliance) should not be a roadblock to productivity.

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Create a plan. Keep it simple. Communicate the plan.

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Hot Topics:

Key concepts that apply to businesses of all sizes.

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Hot Topics:

Top Causes of Data Breaches

July 2021 – January 2022

- Unauthorized Employee Email Account Access
- Unauthorized System Access
- Inadvertent Disclosure
- Compromised Website
- Insider Theft

Data from Office of Cybersecurity & Critical Infrastructure Protection. Listed in order of number of reported incidents.

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Hot Topics:

MFA (Multi Factor Authentication)

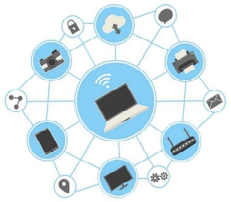
- Is designed to be enable on cloud-based services, remote access, internal admin level accounts.
  - This applies to corporate accounts operated by HR/Marketing/Finance:
    - Facebook, Twitter, Third-Party Financial Accounts, etc.
- Enabling MFA on all personal accounts (especially executive-level personnel where there's a phishing risk) is recommended.
- If you're tired of entering MFA codes, use an authentication app.
  - With an authentication app, you have the option to "approve login" rather than entering a code.
  - Can be configured to only require MFA on first login on a new device.

94% of Ransomware victims did not have MFA in place (Microsoft data)

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Hot Topics:
Encryption

- It's not just for cell phones and laptops.
  - Can be enabled on all storage devices. Laptops, PCs, cell phones, tablets, USB drives, backup devices, servers, cloud services, etc.
- Top 3 reasons why encryption is recommended
  - Encryption is an efficient last line of defense.
  - Encryption protects data on the go.
  - Encryption is a GLBA requirement.



Hot Topics:

Baseline Network Assessment

- Creating a baseline of network traffic (internal and external) provides visibility to unexpected communications.
- Direct external connections via IP addresses should be only permitted by whitelisting.

Hot Topics:

Geolocation Blocking

- If all your employees work in the U.S. and will never login from a foreign country, then you may consider blocking all login attempts from locations external to the U.S.
- Auditing login locations.
- Consider white-listing all outbound traffic to foreign destinations.

Hot Topics:

Air-Gapped Backup

- An air-gapped backup is a copy of your data that is stored on a separate network, uses separate credentials, and is configured so the data cannot be changed. This protects it from ransomware spreading on the local network.

IT Exam Focus Areas:

Cybersecurity Insurance

- If you have a cybersecurity insurance policy:
  - Review the policy – Does it cover acts of war?
  - Build contacts into your Disaster Recovery / Business Continuity Plan.
    - Know who to call in the event of a cyber event.
  - Work with your insurance carrier to have vendors pre-approved for incident response.
  - Ask your carrier to provide a list of best practices to implement.

IT Exam Focus Areas:

Vulnerability Scanning / Patch Management

- In-house vulnerability scanning for all internal scannable assets.
  - Performing regular authenticated and credentialed scans and incorporating the process into the audit/testing plan and remediation process.
- External vulnerability scanning for all external scannable assets.
- Develop a process to ensure findings are documented, assigned for remediation, documented for resolution, and reported to an oversight committee.

IT Exam Focus Areas:

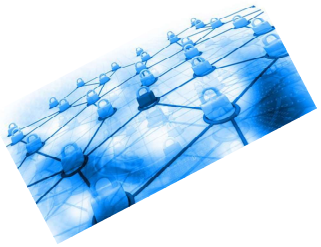
System Hardening

- Some best practices to harden all network devices, servers, desktops, and applications are:
  - Establish a minimum-security baseline/hardening checklists for all systems and applications.
  - Ensuring compliance through a manual validation process or compliance scanning tool (vulnerability scanning).

IT Exam Focus Areas:

Access Control Review

- Regular access reviews for all systems where accounts are created:
  - Examples - Active Directory, Core Data Processing, Cloud Services, etc.
- Use principle of least privilege required.



IT Exam Focus Areas:

Network Segmentation (Micro-segmentation)

- Micro-segmentation is a method of creating network zones in data centers, cloud environments, and on your LAN/WAN to isolate traffic.
- Used to prevent unauthorized access, limit spread of ransomware, and increase auditing functions.

IT Exam Focus Areas:

Training

- Disaster Recovery / Business Continuity
  - Who is doing what and when?
  - Marketing communication plan developed?
- Incident Response
  - Cyber insurance
  - Will you pay ransomware?
- Social Engineering
  - Email
  - Texts
  - Phone calls

IT Exam Focus Areas:

Mobile Device Management

- Mobile device management (MDM) refers to the control of mobile devices through various types of access control and monitoring technologies. It is important for businesses to both allow for effective mobile device use and protect sensitive data from unauthorized access.
  - Provides the ability to enforce encryption, device access codes, manage software on the devices (patch management), remote wipe the device if lost, etc.

IT Exam Focus Areas:

Cyber-Warfare

- Essential Services
  - Identify the minimum state of operations required to maintain essential services.
- Customer Confidence
  - Identify minimum level of service to maintain customer confidence.
- Funds Availability
  - Identify alternate arrangements in the event of payment system disruptions (e.g., cash delivery service, ATM, Electronic banking, mobile banking, etc.).

IT Exam Focus Areas:

Cyber-Warfare

- Bookkeeping Records
  - Identify how your staff will access essential bookkeeping records.
- Critical Infrastructure
  - Senior management and the Board should consider how to address the potential for extended outages of power, telecommunications, and financial market infrastructures.

IT Exam Focus Areas:

Cyber-Warfare

- Technology Service Provider
  - Senior management and the Board should consider how to address the potential for an extended outage of access to data and functionality from your core processor and other technology service providers.
    - A tabletop exercise is an excellent way to engage.

IT Exam Focus Areas:

Bonus Topic: Updates to GLBA

- GLBA was updated in 2021.
- 11 core changes were adopted (some have multiple parts).
  - 9 of the changes take effect December 2022.
  - 2 of the changes took effect December 2021.

IT Exam Focus Areas:
Bonus Topic: Updates to GLBA

- Key changes:
  - The rule now requires designation of a single “qualified individual” to be responsible for the security program.
  - The update includes more specific criteria for what the risk assessment must include.
    - Criteria for evaluating and categorizing of security risks and threats.
    - Criteria for assessing the adequacy of security safeguards.
    - How identified risks will be mitigated or accepted.
    - The risk assessment must be in writing.

IT Exam Focus Areas:

Bonus Topic: Updates to GLBA

- Key changes (continued):
  - Numerous changes to Security Safeguards (not all listed):
    - Access controls (least privilege required)
    - Physical access controls
    - Access reviews
    - Inventory and classification of data, devices, and systems
    - Encryption of customer information at rest and in transit over external networks

IT Exam Focus Areas:
Bonus Topic: Updates to GLBA

- Key changes (continued):
  - Numerous changes to Security Safeguards (not all listed):
    - Multi-factor authentication (required)
    - Change management procedures
    - Monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users

IT Exam Focus Areas:

Bonus Topic: Updates to GLBA

- Key changes (continued):
  - Regular testing of safeguards must now include either continuous monitoring or periodic penetration testing (annually) and vulnerability assessments (biannually).
  - Financial institutions must now provide security awareness training and updates to personnel.
  - Periodically assess service providers based on the risk they present and the continued adequacy of their safeguards.

IT Exam Focus Areas:
Bonus Topic: Updates to GLBA

- Key changes (continued):
  - The Final Rule requires financial institutions develop incident response plans "designed to promptly respond to, and recover from, any security event materially affecting . . . customer information in their control."
  - The rule requires a financial institution's CISO/Qualified Individual to report in writing regularly, and at least annually, periodic reports to a Board of Directors or governing body.

IT Exam Focus Areas:

Bonus Topic: Updates to GLBA

- Key changes (continued):
  - Financial institutions must regularly test or monitor the effectiveness of the security safeguards and make adjustments in light of the results of the testing and monitoring. (Effective now)
  - The FTC update expands on the definition of "financial institution" to require "finders" — companies that bring together buyers and sellers — to follow the Safeguards Rule. (Effective now)

Compliance is a journey, not a destination.

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES

Thank You
Questions?

Jake Martin
Cybersecurity & IT Resource Specialist
Michigan Department of Insurance and Financial Services
Tel:517-230-5533
MartinJ47@michigan.gov

DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES
www.michigan.gov/DIFS
877-999-6442
@MIDIFS MIDIFS