2019 Annual Leadership Conference
September 25 -27, 2019

Staying at the Forefront of Cybersecurity Threats

Presented by:
John Hock, CPA, CITP, CISA, SOC
IT Audit Manager

MACUMA
Metropolitan Area Credit Union Management Association

Objectives

- How scary is it?
  - Pervasiveness
  - Cost
- Identify cybersecurity threats and risks
  - Assess risk
- What can we do about it?
  - Budget and strategy
  - Board's role in cybersecurity

How Scary Is It?

MACUMA
Metropolitan Area Credit Union Management Association

How Scary Is It? – Pervasiveness

143 million identities

5 million debit and credit cards

How Scary Is It – Pervasiveness

- Yahoo had 2 breaches – over 3 billion users affected
- 383 million records breached at Marriot in 2018
- 184 million records stolen in connected Facebook incident in 2018
- 2 million customers had PII hacked in T-Mobile breach in 2018
- 147.9 million consumers affected by Equifax breach
- 100k groups and more than 400k machines affected by WannaCry in 2017 ($4 billion in costs)

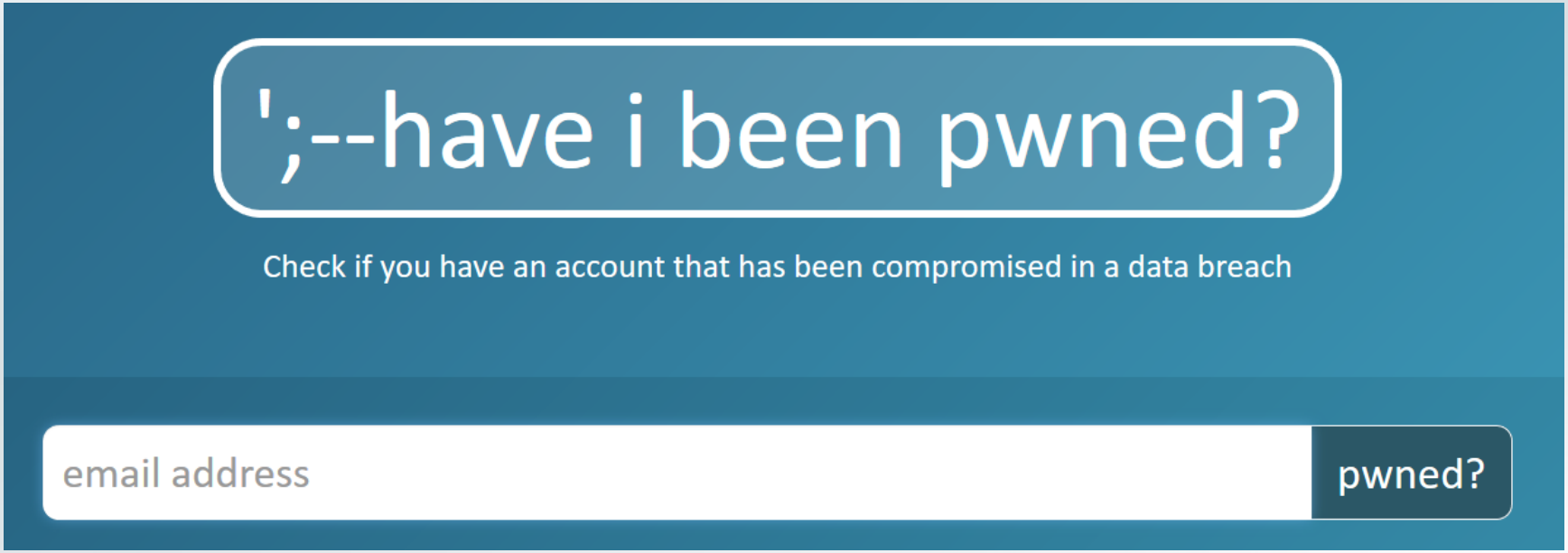
How Scary Is It – Pervasiveness

- Wendy's paid $50m in data breach case to CUs from 2016 hack
- BSA officers targeted by malware-filled phishing attacks in 2019
- 150 million My Fitness Pal (Under Armor) accounts hacked in 2018
- Sheffield Credit Union (UK) attack leaked info on 15k members through brute force password attack
- Hackers breached Virginia Bank twice in 8 months ($2.4m stolen by malware)

- Video games, novelties, messaging apps, and more

How Scary Is It? – Pervasiveness

- Wondering if you have been compromised?



How Scary Is It? – Pervasiveness

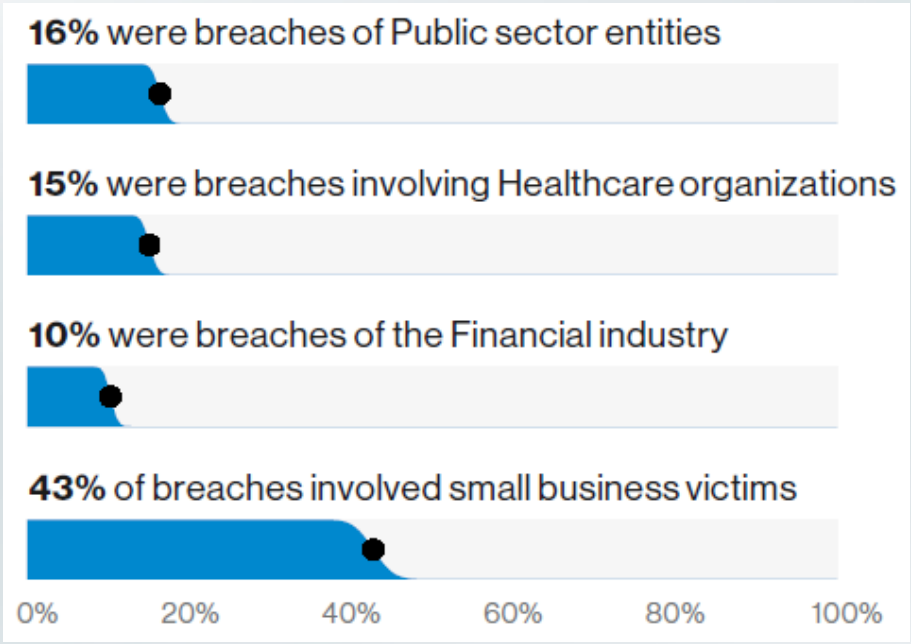
There is no such thing as a 100% secure system

How Scary Is It? – Pervasiveness

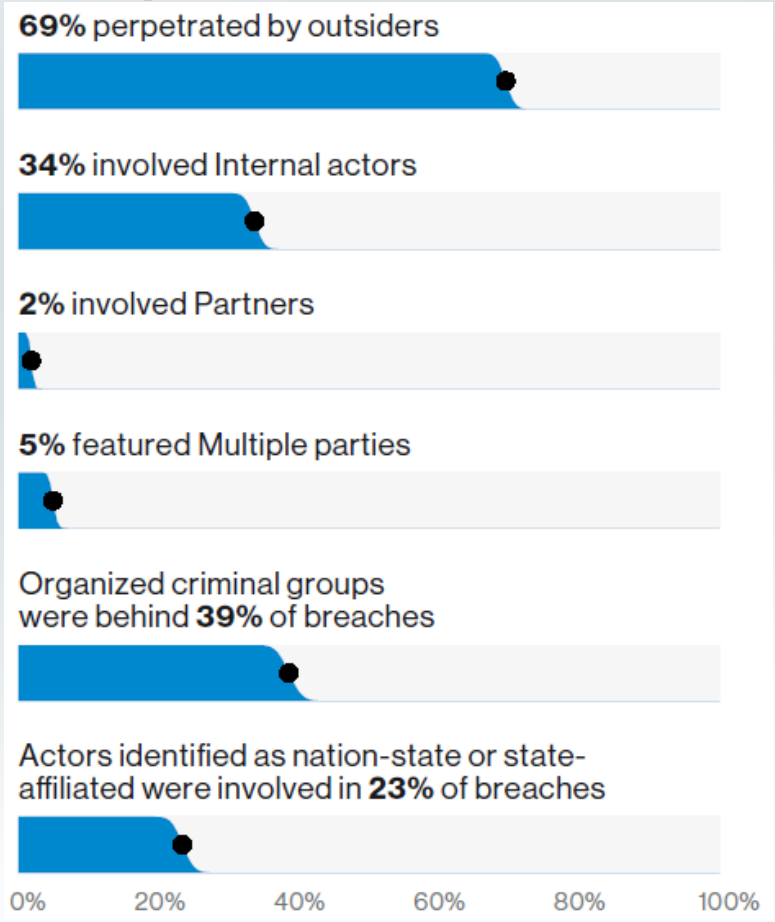
- Summary of Ponemon's 2018 State of Cybersecurity in SMBs
  - **Phishing attacks** increasing to 52% of SMBs
  - **Negligent employees** or contractors rose to 60% of breaches
  - Exploits and malware are **evading** intrusion detection (72%) and anti-virus solutions (82%)
  - **Ransomware** increased to 61% of respondents, 70% of which paid
  - Businesses are losing more **records** (11k from 9k)
  - More **mobile devices** are being used to access business critical apps and IT infrastructure (45%)

How Scary Is It? – Pervasiveness

Victims



Perpetrators

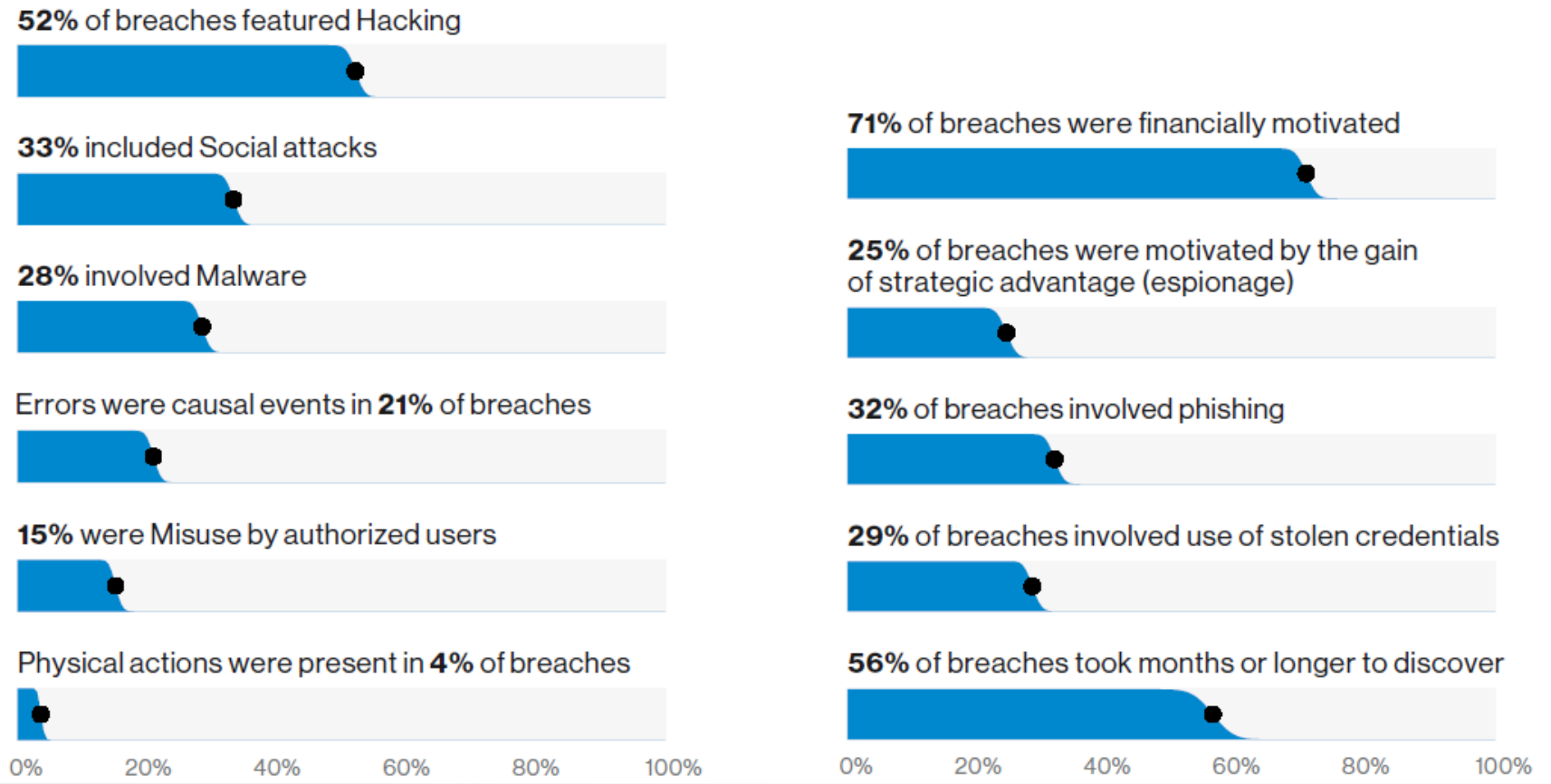


How Scary Is It? – Pervasiveness

- 71% of breaches were **financially motivated** (76% in 2018)
- 69% of cyberattacks were perpetrated by **outsiders** (73% in 2018)
- 34% of attacks involved **insiders** (28% in 2018)

How Scary Is It? – Pervasiveness

Tactics and common elements



Threat Actors

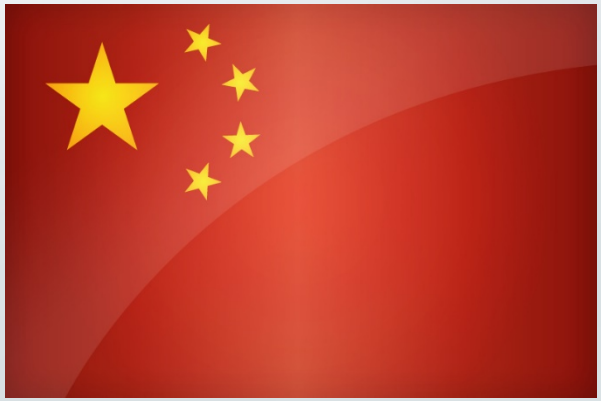
- Hackers
  - There is a hacker attack every 39 seconds.

Source: University of Maryland A. James Clark School of Engineering Study

- Kaspersky Labs
- FireEye Cyber Threat Map

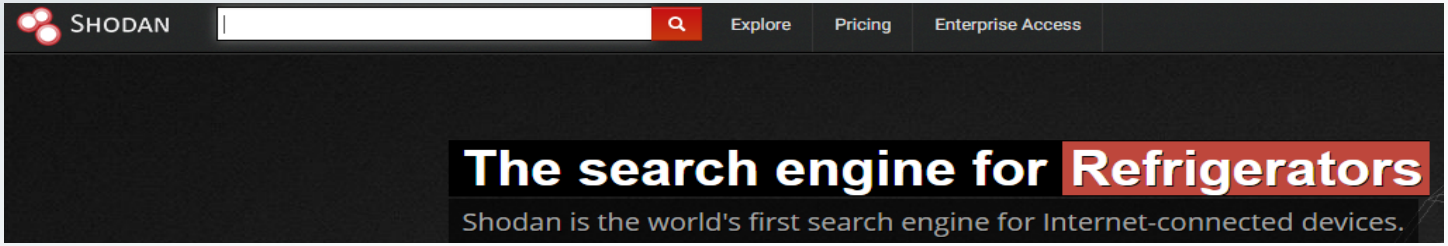
Threat Actors

- Nation-states
  - China
  - Russia
- Terrorists
- Criminal enterprises



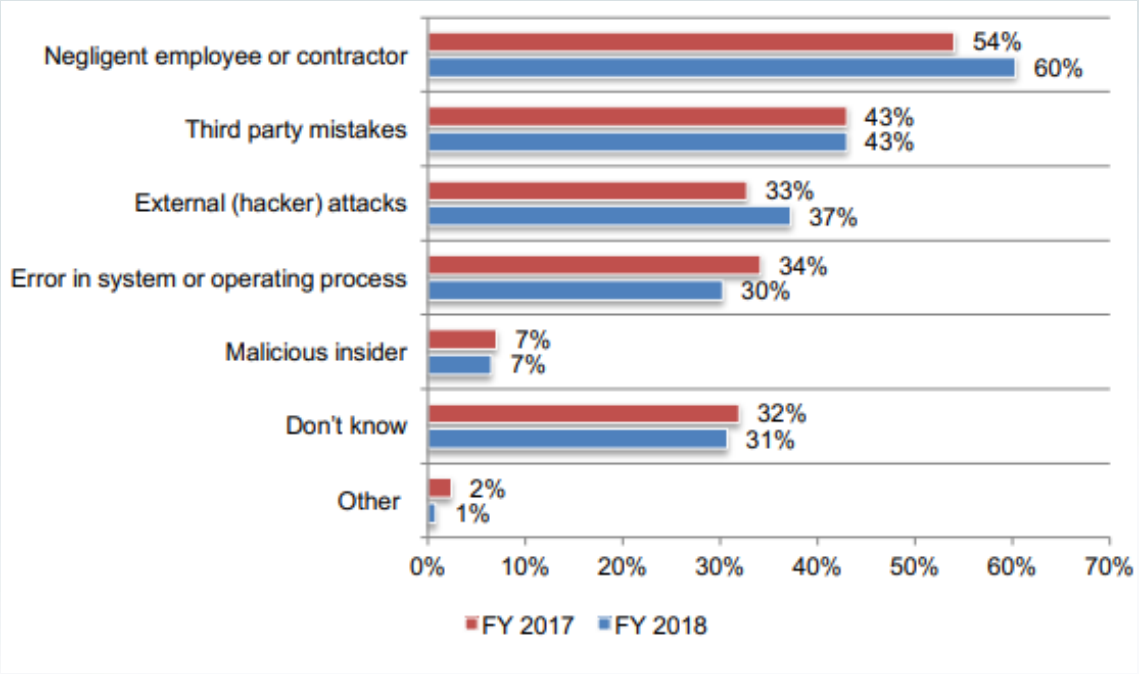
How Scary Is It? – Pervasiveness

- What is causing the increased rate of attacks?
  - Access to larger systems
  - Cyber extortion or ransomware
  - Data is easier to sell (private, personal, financial)
  - Tools are cheap and readily available
  - It is fun and easy (exploit-db.com and shodan.io)

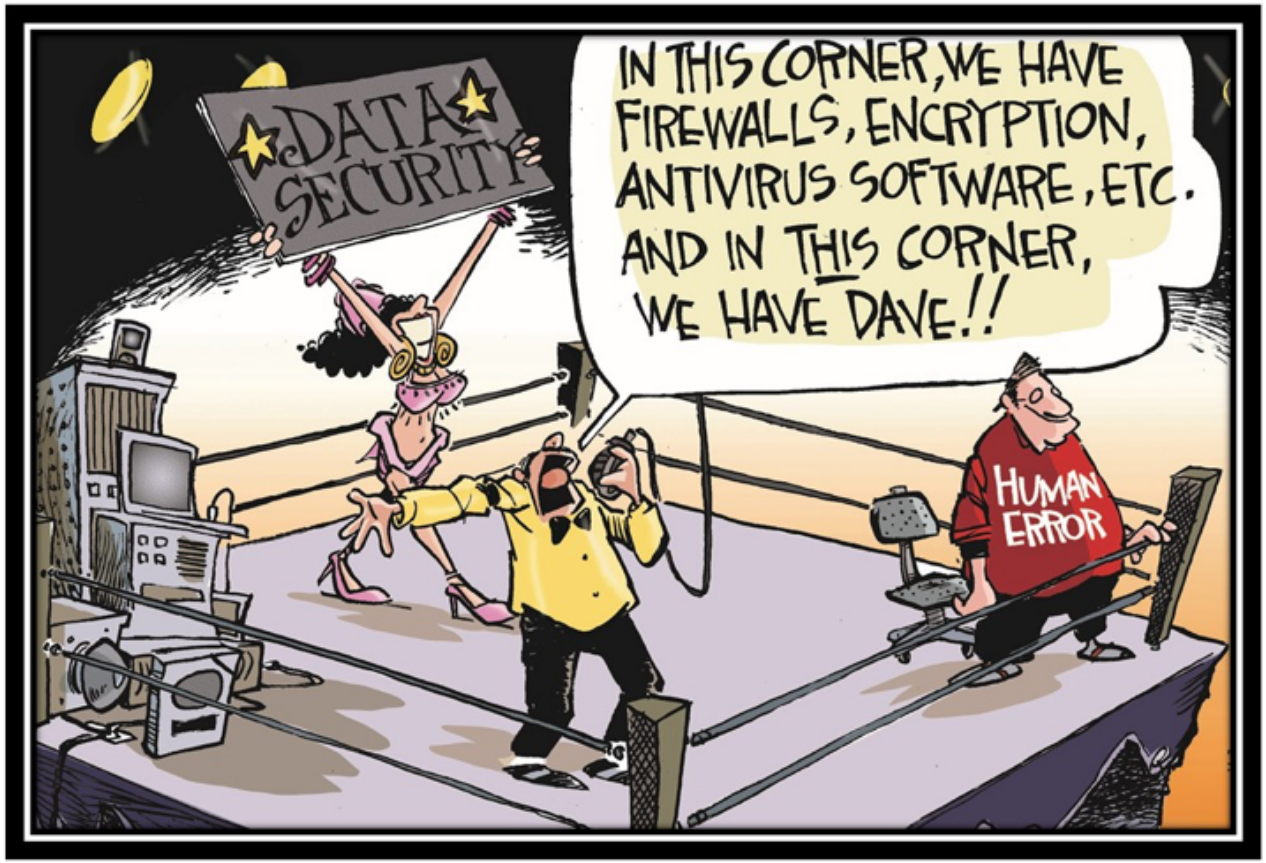


How Scary Is It? – Pervasiveness

- What was the root cause of data breach?
  - Our **people** are still the largest risk
  - Due diligence on **third-parties** still front and center
  - One third could not determine



Employees


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

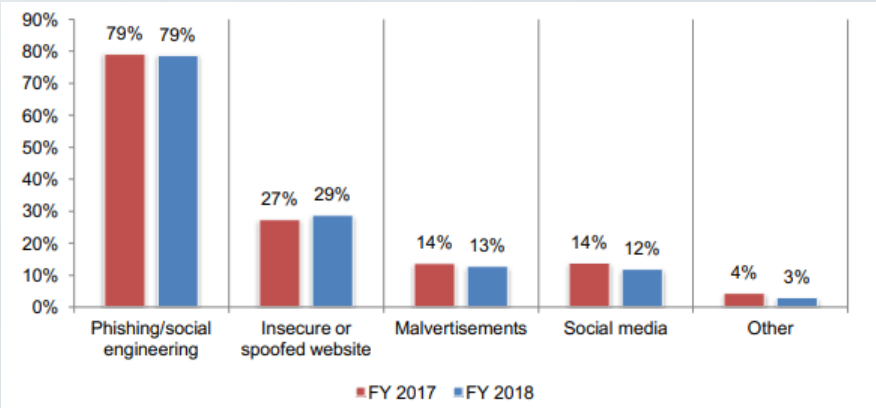
Employees

- Errors were at the heart of almost one in five (17%) breaches
- That included:
  - Employees failing to shred confidential information
  - Sending an email to the wrong person
  - Misconfiguring web servers

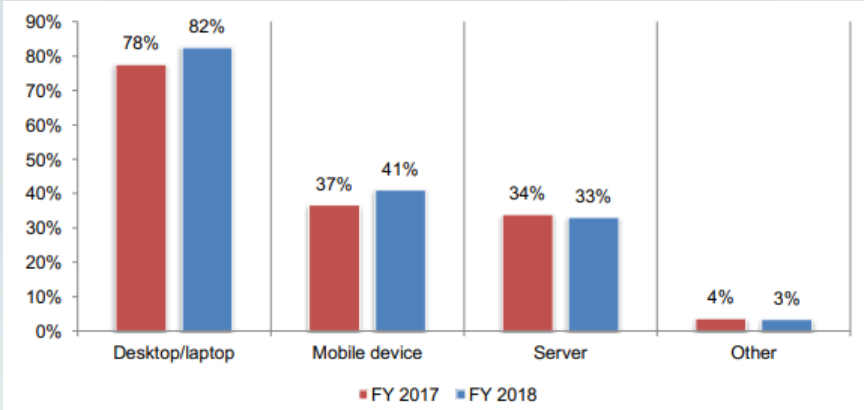
Source: Verizon 2018 DBIR

How Scary Is It? – Pervasiveness

How was ransomware unleashed?



Where was ransomware unleashed?



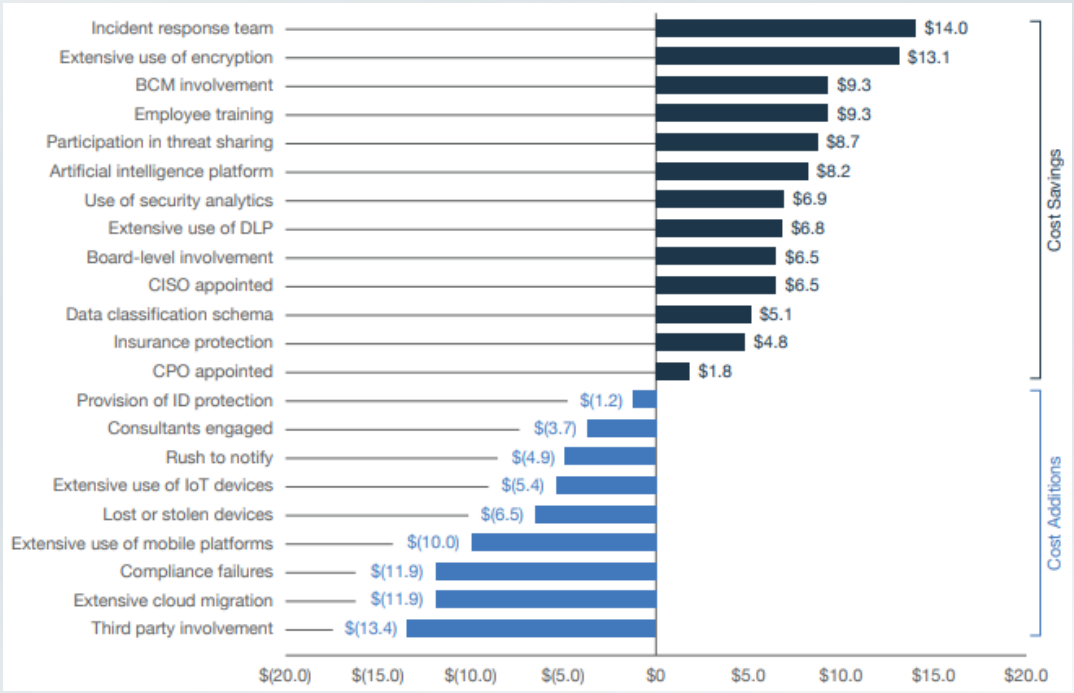
How Scary Is It? – Cost

- Per the 2019 Cost of Data Breach Study, the average cost of a data breach is currently $3.9 million.
- On average in the financial services industry the cost is $210 per record compromised.
- Companies with an incident response team saved an average of $360,000

Source: 2019 Cost of a Data Breach Report

How Scary Is It? – Cost

- What affects the cost?
  - Incident response team and extensive encryption save the most
  - Compliance failures and extensive mobile/IoT can add considerably



How Scary Is It? – Cost

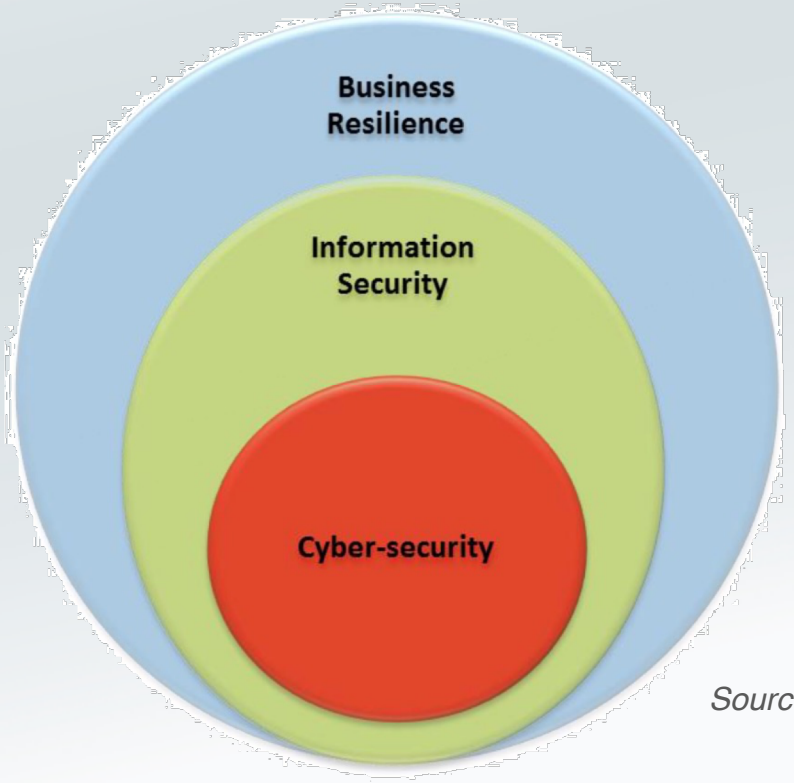
- What are some of the surprise costs?
  - Organizational changes and process fixes
  - Additional training
  - Remediation to recover data
  - Good will incentives to keep customers
  - Increased cyber insurance premiums
  - Member loyalty lowered

Identify Cybersecurity Risk

MACUMA
Metropolitan Area Credit Union Management Association

Cybersecurity

The ability to protect or defend the use of cyberspace from cyber attacks.



Source: CNSSI-4009 - NIST.IR.7298r2

Risk Assessment Quality

- Consider the issues identified in the assessments.
- Discuss the contents of the risk assessment.
- Consider:
  - Reliance on technology
  - Presence of member data
  - Regulations
  - Risk mitigation

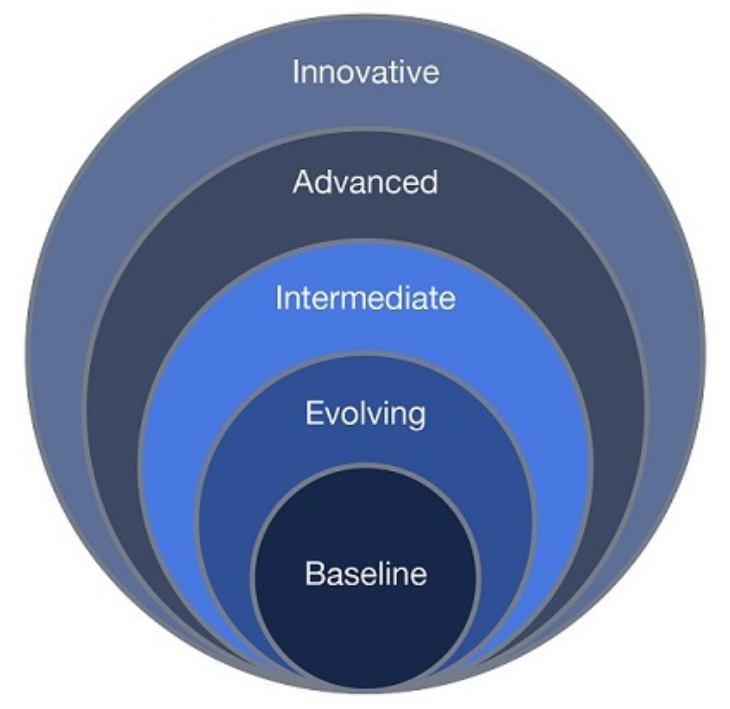
Cybersecurity Assessment Tools

MACUMA

Metropolitan Area Credit Union Management Association

Cybersecurity Assessment

- NCUA's Automated Cybersecurity Examination Tool (ACET)
  - Repeatable, measurable, transparent
  - **Mirrors CAT** (Inherent Risk and Cyber Maturity) with additional features
  - Statements in **five domains**
  - Mapped to FFIEC IT Exam Handbook, regs, and NIST Cybersecurity Framework
  - Does **not** replace GLBA risk assessment requirement
  - **Voluntary**, but recommended



Benefits to the Institution

- Enhanced oversight and management of the institution's cybersecurity:
  - Identifying factors contributing to and determining the institution's overall cyber risk.
  - Assessing the institution's cybersecurity preparedness.
  - Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
  - Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
  - Informing risk management strategies.

Assessment Components

- The assessment consists of two parts:
  - Inherent risk profile
  - Cybersecurity maturity
- Benefit
  - Upon completion of both parts, management can evaluate whether the institution's inherent risk and preparedness are aligned.

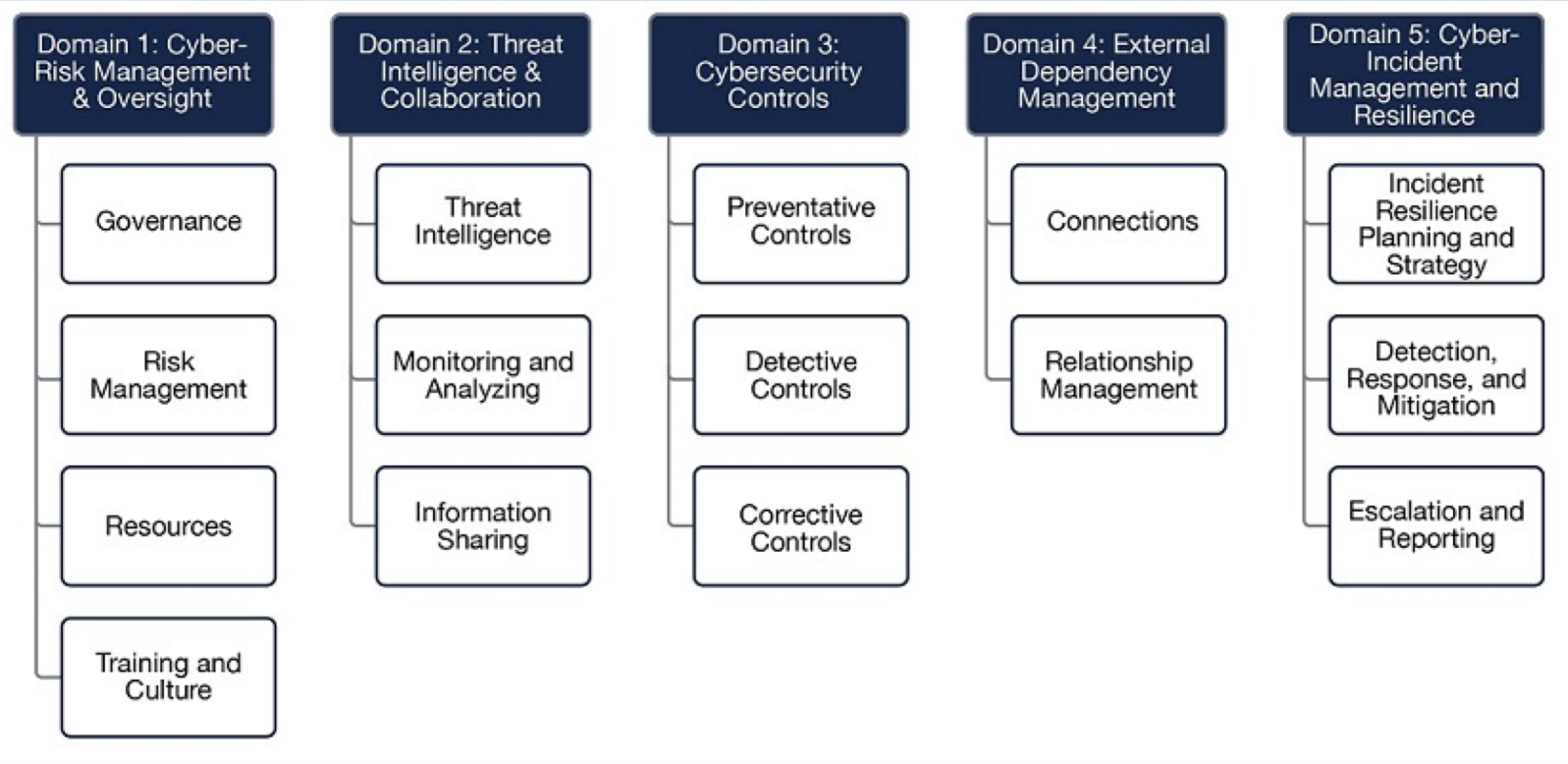
Inherent Risk Profile

- Cybersecurity inherent risk is the level of risk posed to the institution by the following:
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats
- Inherent risk does not include mitigating controls.

Inherent Risk Profile (IRP)	Inherent Risk Level					Total Items	Risk Level
	1	2	3	4	5		
Category							
Technologies and Connection Types	7	7	0	0	0	14	2 - Minimal
Delivery Channels	2	1	0	0	0	3	1 - Least
Online/Mobile Products and Technology Services	4	8	2	0	0	14	2 - Minimal
Organizational Characteristics	1	5	1	0	0	7	2 - Minimal
External Threats	0	1	0	0	0	1	2 - Minimal
Total	**14**	**22**	**3**	**0**	**0**	**39**	

Cybersecurity Maturity

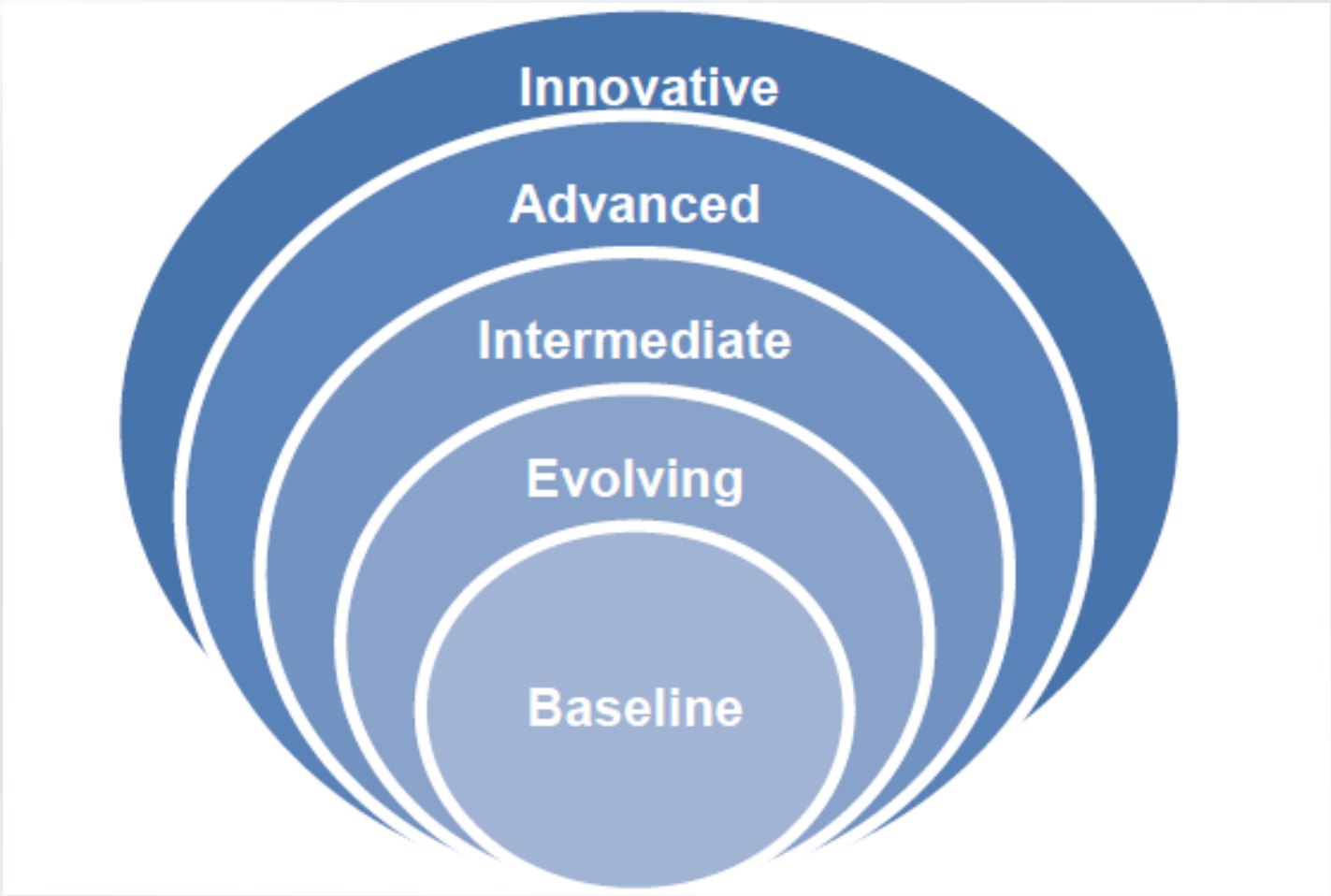
- Management then evaluates the institution's cybersecurity maturity level for each of five domains:



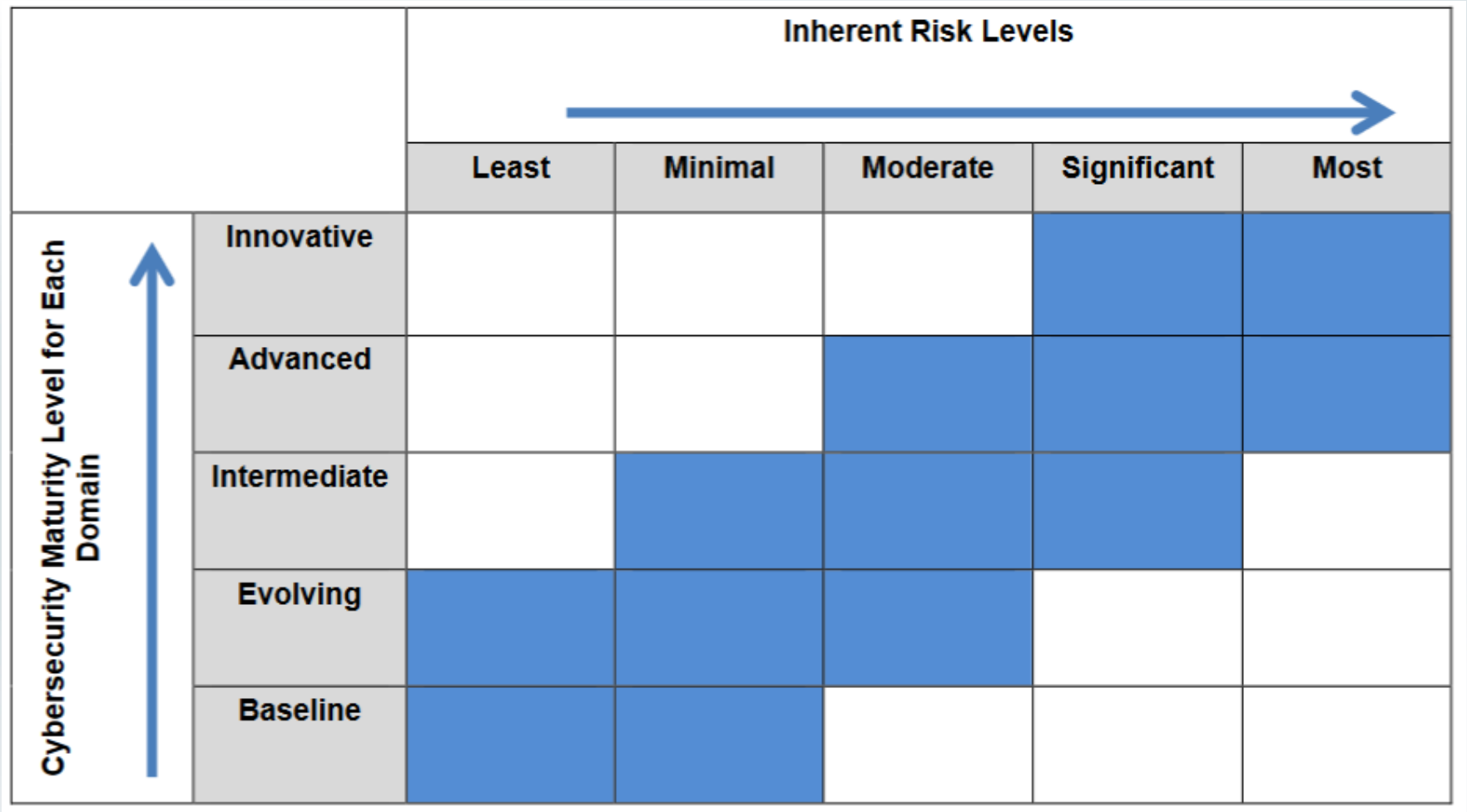
Five Key “Domains” for Cybersecurity Preparedness

1. Cyber risk management and oversight
   - Strong governance is essential
2. Threat intelligence and collaboration
   - Strength in numbers
3. Cybersecurity controls
   - More than one kind of control
4. External dependency management
   - Your security starts with their security
5. Incident management and resilience
   - Mitigation and recovery are a must

Maturity Levels



Risk / Maturity Relationship



The Role of the Board

Or an **appropriate board committee**:

- Engage management in establishing the institution's vision, risk appetite and overall strategic direction.
- Approve plans to use the assessment.
- Review management's analysis of the assessment results, inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results.
- Review management's determination of whether the institution's cybersecurity preparedness is aligned with its risks.
- Review and approve plans to address any risk management or control weaknesses.
- Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.

Maturity Levels: Defined

Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

The Board of Directors Role in Cybersecurity

MACUMA
Metropolitan Area Credit Union Management Association

Board of Directors

- Ultimately responsible for member's data
  - Board chair must certify compliance with Part 748 each year in the Report of Officials.
- Everyone is responsible for security!

Board of Directors

- Engage vision, risk appetite and overall strategic direction.
- Oversee the cybersecurity assessment, its results, inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results.
- Review whether cybersecurity preparedness is aligned with risks.
- Review and approve plans to address any risk management or control weaknesses.
- Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.

Board of Directors

- Create a culture of cyber security awareness
  - Advocate for progressive, ongoing training and messaging to ensure the whole institution is prepared

Board of Directors

- Advocate people-centric security training.
  - Jane and Dolores do not need to be trained the same
  - Effective use of training dollars

Board of Directors

- Approve information security policy and advocate a strong security culture.
  - Determine adequacy of policy based on size and technical complexity

Managing Risk

MACUMA
Metropolitan Area Credit Union Management Association

Cyber Risk Mitigation

- Change risk profile (streamline risk)
- Increase cybersecurity investment (staff, infrastructure, services)
- Increase capital (accept the risk)
- Alternative risk management approaches
- Cyber insurance (insure what you can't control)

What can we do about it?

- Best practices of high performing institutions
  - Higher budgets and in-house expertise are key
  - Strong passwords and/or biometrics
  - Password policies
  - Detailed and updated incident response plan

What can we do about it?

- Increasing use of managed security service providers (MSSPs)
  - Firewalls or intrusion prevention
  - Intrusion detection
  - Security gateways (messaging or web)
  - Vulnerability scans
  - Identity and access management
  - Analysis and reporting of events

What can we do about it?

- Increasing use of managed security service providers (MSSPs)
  - Firewalls or intrusion prevention
  - Intrusion detection
  - Security gateways (messaging or web)
  - Vulnerability scans
  - Identity and access management
  - Analysis and reporting of events

Cybersecurity Professionals

- Independent or third-party tests
  - Internal and external vulnerability scans (credentialed)
  - Penetration testing (more than 20 hours)
  - Phishing and other social engineering campaigns
  - Full logical access testing and segregation of duties
  - GLBA, FFIEC, general controls, application controls

Cyber Insurance

- FFIEC Joint Statement, April 2018
  - Cyber Insurance and Its Potential Role in Risk Management Programs
- “To provide awareness of the potential role of cyber insurance in financial institutions’ risk management programs.”

Cyber Insurance

- According to the FFIEC, cyber insurance is not a regulatory requirement
- May offset financial losses resulting from cyber incidents

Cyber Insurance

- According to the FFIEC, purchasing cyber insurance does **not** remove the need for a sound control environment.
- Traditional insurance policies for general liability or basic business interruption coverage may not fully cover cyber risk exposures without special endorsement or by exclusion not cover them at all.
- Coverage may also be limited and not cover incidents caused by or tracked to outside vendors.

Resources

- NCUA Cybersecurity Resources
  - https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/resource-centers/cyber-security.aspx
- National Institute of Standards and Technology
  - https://www.nist.gov/topics/cybersecurity
- SANS Institute
  - https://www.sans.org/security-resources/
- Federal Financial Institutions Examination Council
  - https://www.ffiec.gov/cybersecurity.htm

Thank You!

John Hock
CPA, CITP, CISA, SOC
IT Audit Manager
Hock@doeren.com
248-535-8650