Cybersecurity Threats & Resiliency

Introduction

What is a Cybersecurity Practice Leader anyway?

01

Geek to English

Quick guide to important cyber and tech terms

02

2021 No Lockdown for Data Breaches

Incidents, Breaches, and Claims didn't pause for the pandemic!

03

Becoming Resilient

Adding resiliency to your technology operation

04

Resources

MMRMA & the Cybersecurity community are here for you and your team

05

Questions & Answers

Here you could describe the topic of the section

06

Cybersecurity Practice Leader

Visions, engineers, and executes cybersecurity risk management endeavors and provides members with relevant guidance and thought leadership in cybersecurity policies, practices, and innovation opportunities. Serves as a cybersecurity subject matter expert in support of the mission of Michigan Municipal Risk Management Authority.

Introduction

Education

2+ years

2FA, Network security & Employee training

Local Government

9+ years

Successful defense against Ransomware

Financial Services

6 years

International Trade Services Cyber & OFAC compliance

Federal Government

2 Years

Messaging & Signal encryption and Cybersecurity

Manufacturing

3 years

Network & Endpoint Security & data exchange & storage

Healthcare

5 Years

Network security design & messaging security & HIPAA Compliance

Introduction

What is a Cybersecurity Practice Leader anyway?

01

Geek to English

Quick guide to important cyber and tech terms

02

2021 No Lockdown for Data Breaches

Incidents, Breaches, and Claims didn't pause for the pandemic!

03

Becoming Resilient

Adding resiliency to your technology operation

04

Resources

MMRMA & the Cybersecurity community are here for you and your team

05

Questions & Answers

Here you could describe the topic of the section

06

Terminology

Incident

- An incident is any event outside of normal operations that interferes with, or disrupts, processes necessary to organizational operations.
- An example: You get a verification code from Duo that you didn't request, or you lost your laptop and cannot find it.

Breach

- A breach is any incident that results in loss or unauthorized access to an organization's network, data, applications, or devices.
- An example: After a successful phishing attack, your organization is hacked, and sensitive information is released.

Ransomware

Malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

Typical Attack Chain

Introduction

What is a Cybersecurity Practice Leader anyway?

01

Geek to English

Quick guide to important cyber and tech terms

02

2021 No Lockdown for Data Breaches

Incidents, Breaches, and Claims didn't pause for the pandemic!

03

Becoming Resilient

Adding resiliency to your technology operation

04

Resources

MMRMA & the Cybersecurity community are here for you and your team

05

Questions & Answers

Here you could describe the topic of the section

06

2021 Cyber Insurance Claims Report

- Cyber crime is unprecedently increasing.
- Ransomware is growing in severity.
- Criminals are taking advantage of dislocations in how we work.
- The rush to facilitate remote work has come at a large cost.
- Smaller companies are increasingly targeted.

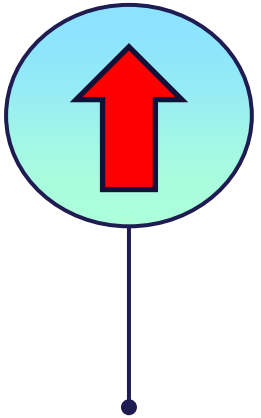
Cybercrime is increasing

51%

Business email Compromise

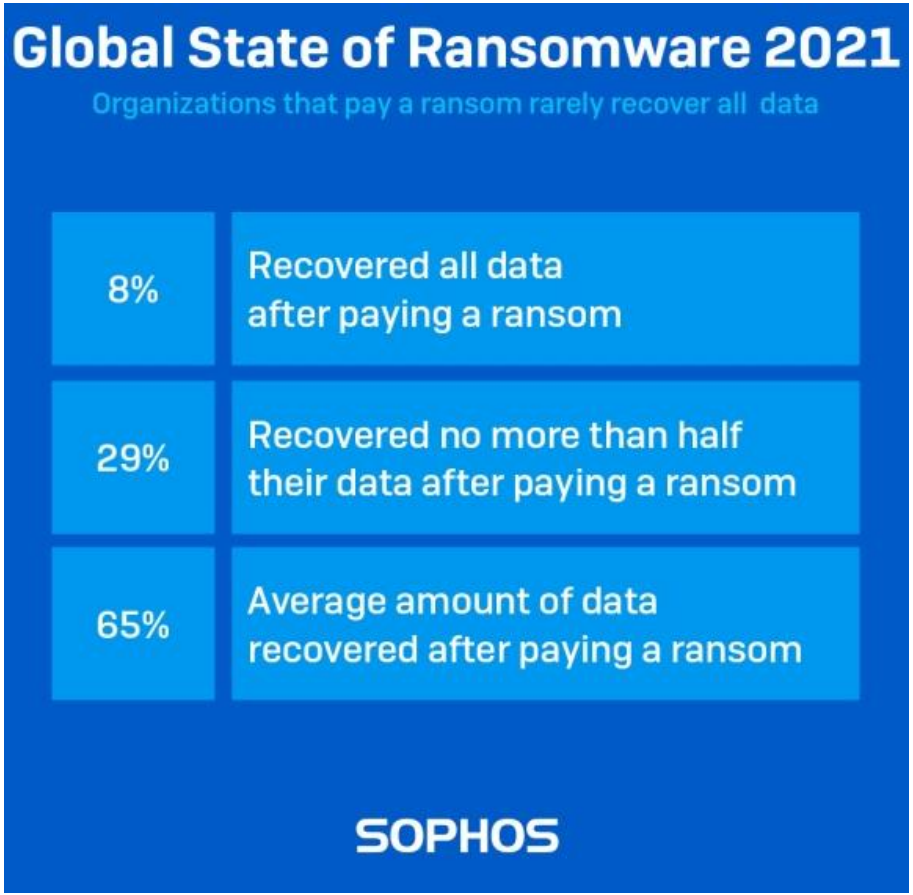
Funds Transfer Fraud

28%



Ransomware Severity

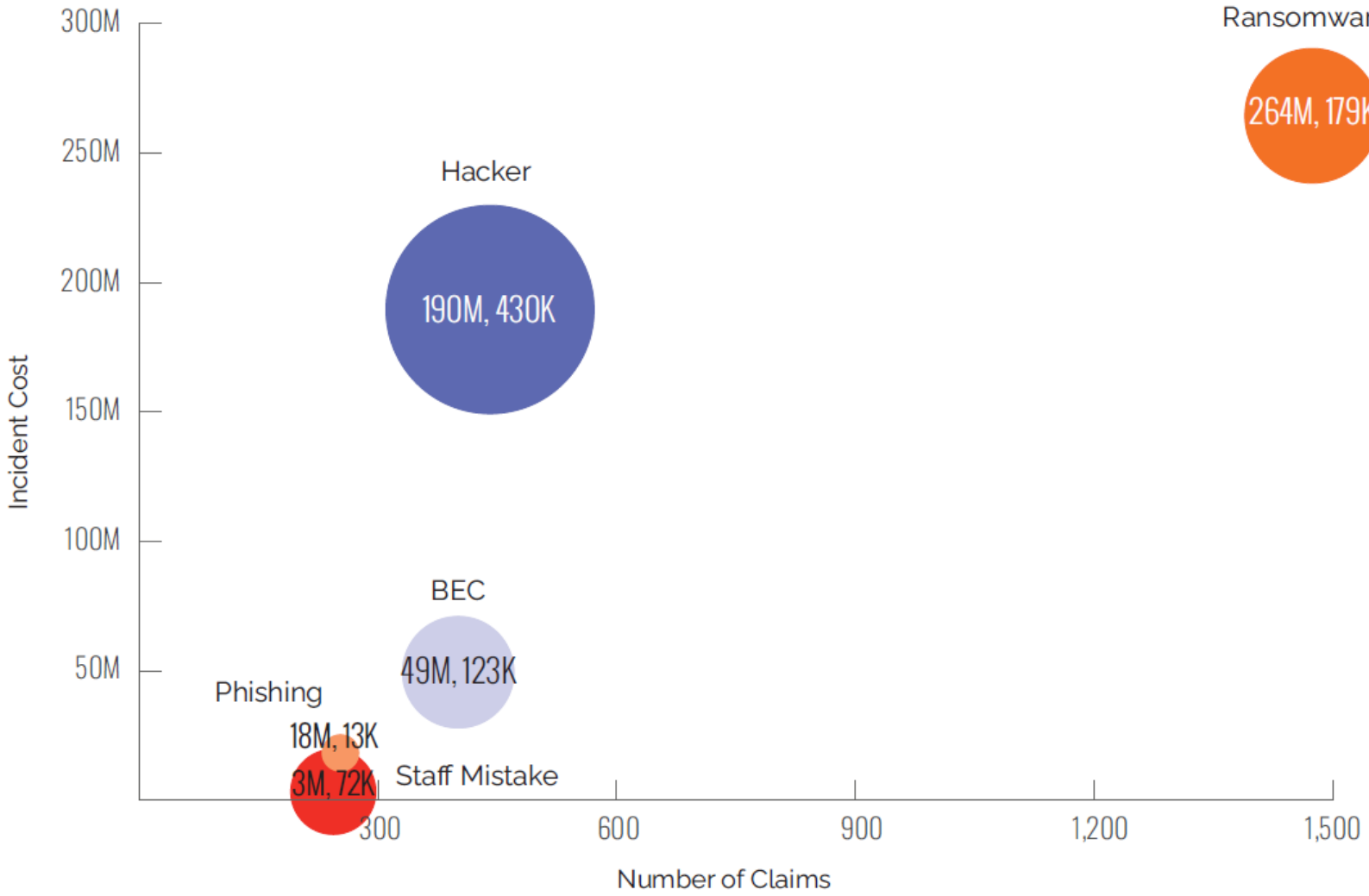
Ransomware volume down severity up



The average ransom paid by mid-sized organizations was US$170,404.

The average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was US$1.85 million.

Encryption is down. Extortion is up.


Ransomware
264M, 179K
Hacker
190M, 430K
BEC
49M, 123K
Phishing
18M, 13K
Staff Mistake
3M, 72K
300M
250M
200M
150M
100M
50M
Incident Cost
300
600
900
1,200
1,500
Number of Claims

Pandemic of FTF's

Contributors to Funds Transfer Fraud

- **Increased remote work means fewer in-person interactions**
- **Increased use of electronic funds transfers**
- **Changes to operational structures, processes, and policies**

RESULTS

- **179% INCREASE in the average amount stolen**

The Rush to Remote Came At A Cost

Speed v. Security

The Pandemic was sudden
The deployment of remote work tools was faster
Skills & Secure configuration has lagged

Cyber Criminals Pounced

Attack severity rose 103% in 2021
Use of vulnerable remote tool up 11%

Too small to notice?

Organizations with under 250 employees increased 57% from the first half of 2020 to 2021.

Automated attacks have become more profitable for criminals to target more small and midsize organizations.

Ransomware as a service (RaaS)

Introduction

What is a Cybersecurity Practice Leader anyway?

01

Geek to English

Quick guide to important cyber and tech terms

02

2021 No Lockdown for Data Breaches

Incidents, Breaches, and Claims didn't pause for the pandemic!

03

Becoming Resilient

Adding resiliency to your technology operation

04

Resources

MMRMA & the Cybersecurity community are here for you and your team

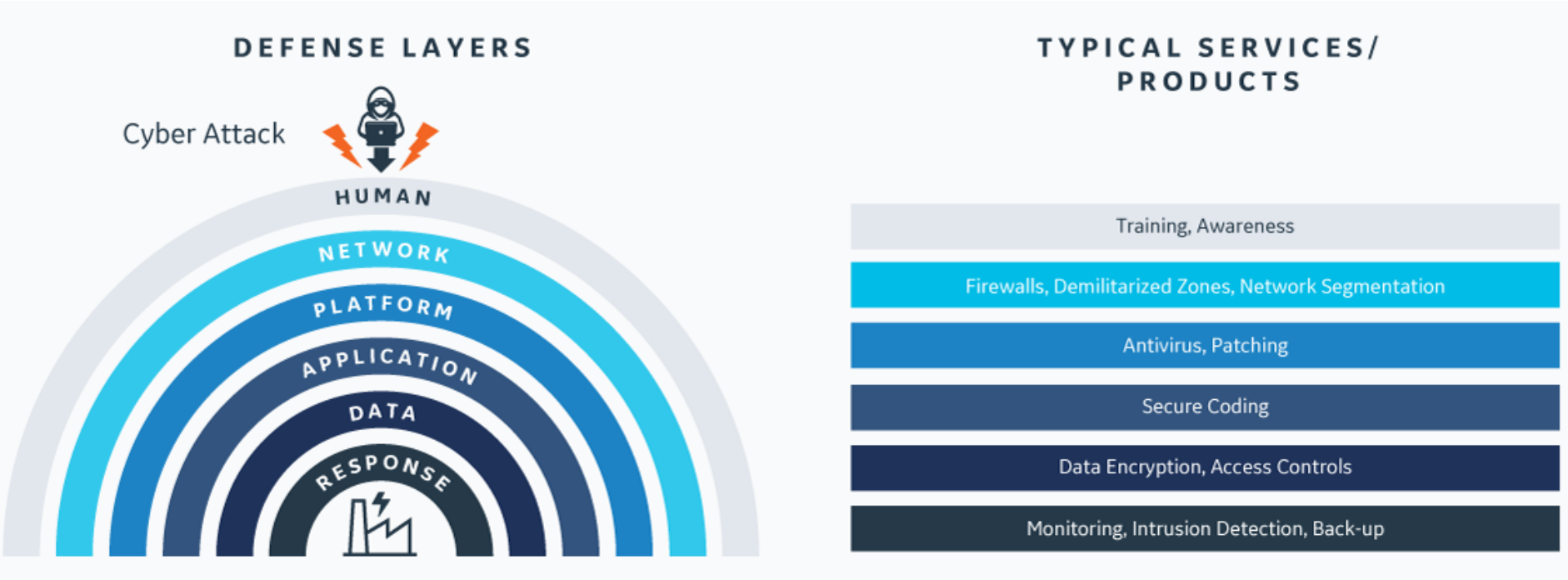
05

Questions & Answers

Here you could describe the topic of the section

06

PREVENT: Traditional Pathways

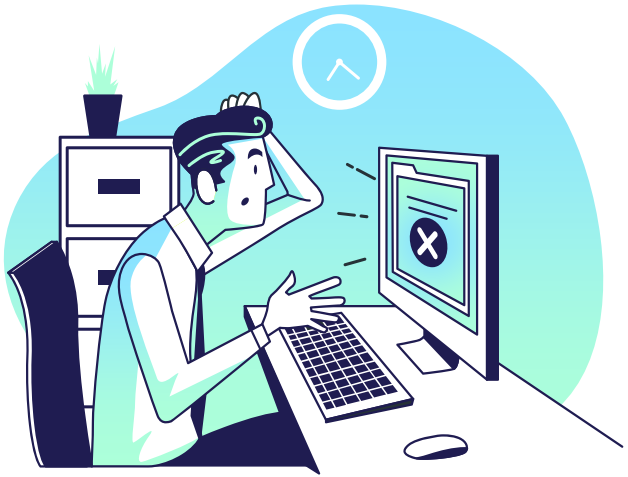


90%

Data breaches began with phishing

Cisco 2021 Cybersecurity Threat Trends Report

PREVENT: Hygiene isn't just for Pandemics!



More than 55,000 known vulnerabilities in commonly used software and systems.

IBM has calculated that breaches of these vulnerabilities cost large enterprises $3.92 million on average;

for 60% of those breaches, patches were available but not applied.

PREPARE: for a Cybersecurity Assessment

A cybersecurity assessment examines a company's information technology infrastructure as well as its security-related policies and practices.

It evaluates:

- **Existing protective systems**
- **Compliance with security regulations**
- **Vulnerability to security incidents**
- **Resilience against potential harm**

PREPARE by completeing a Cybersecurity Assessment

2. Update/Categorize

Spend time **BEFORE** the assessment updating tech diagrams and asset lists and ensure policies and business process documentation is also updated.

3. **Scope**

Define the scope and cost to make the assessment practical and potentially provides a reasonable set of actionable items. Assessment should align to one of the recognized standards: NIST, CIS, ISO27000, COBIT.

1. Assemble!

Make sure the team represents the real risk areas in the organization – not just the technology team.

4. **Prepare for Failure**

Resist the urge to place blame. Focus on the opportunities and the identified successes.

CONTINUE: Acquire, Design and Test Recovery

Acquiring Strong Business Continuity Solutions. A successful plan for resilience requires having the right tools. Business continuity solutions like remote data backups or secondary production environments

Continuously Revising Resilience Plans. Cyber threats are constantly changing. So, it’s important to continuously review and revise resiliency plans

CONSTRAIN: The Attack with Automation

- Security Information and Event Management or SIEM Tools
- Machine Learning (ML)
- Artificial Intelligence (AI)
- SECaaS – Security as a Service

TRANSFORM: Your Cybersecurity Culture

- Add cybersecurity requirements, qualifications, and performance metrics into every RFP and acquisition
- Invest in **PEOPLE** and **APPLIANCES** and **SERVICES** frequently
- Treat Cybersecurity like smoke detector batteries – test and update both at least twice per year
- Create a culture of self-reporting without fear
- Make decisions, policies, and investments based on comprehensive frameworks

SENATE BILL NO. 672

A bill to amend 2004 PA 452, entitled
"Identity theft protection act,"
(MCL 445.61 to 445.79d) by amending the title, as amended by 2006 PA 566, and by adding section 12c.

October 05, 2021, Introduced by Senators SCHMIDT, HOLLIER, HORN, BULLOCK and VANDERWALL and referred to the Committee on Energy and Technology.

Provides for certain affirmative defenses in data breach situations if the covered entity established, maintained, and reasonably complied with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and personal identifying information that reasonably conforms to the current version of an industry-recognized cybersecurity framework or standard described in subsection (2).

Introduction

01

What is a Cybersecurity Practice Leader anyway?

Geek to English

02

Quick guide to important cyber and tech terms

2021 No Lockdown for Data Breaches

03

Incidents, Breaches, and Claims didn't pause for the pandemic!

Becoming Resilient

04

Adding resiliency to your technology operation

Resources

05

MMRMA & the Cybersecurity community are here for you and your team

Questions & Answers

06

Here you could describe the topic of the section

MMRMA

- CYBER@MMRMA.ORG
- RAP Grants (Standard)
  - 2 Factor / Multi Factor Auth 50%/$10k
  - Vulnerability Assessment 50%/$10k
  - Cyber training 50%/$25k
- RAP Grants (Other/Innovative Grant)
- CAP Grants
- RECTify Grants (15k aggregate)
  - 100%/$5k
  - 75%/$5k
  - 50%/$5k
- MMRMA.ORG

RISK

MICHIGAN MUNICIPAL
RISK MANAGEMENT
AUTHORITY

Other Trusted Resources

CISA
CYBER+INFRASTRUCTURE

NVD

HSIN
HOMELAND SECURITY INFORMATION NETWORK
The Trusted DHS Information Sharing Environment

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

NIST
National Institute of Standards and Technology

Introduction

What is a Cybersecurity Practice Leader anyway?

01

Geek to English

Quick guide to important cyber and tech terms

02

2021 No Lockdown for Data Breaches

Incidents, Breaches, and Claims didn't pause for the pandemic!

03

Becoming Resilient

Adding resiliency to your technology operation

04

Resources

MMRMA & the Cybersecurity community are here for you and your team

05

Questions & Answers

Here you could describe the topic of the section

06

THANKS!

Do you have any questions?

Dan Bourdeau
Cyber Practice Leader
CYBER@mmrma.org
(M) 313.495.6830
(O) 734.437.5003

RISK

MICHIGAN MUNICIPAL
RISK MANAGEMENT
AUTHORITY

MMRMA.ORG