CRMWG

Cyber Resilient Massachusetts Working Group

MassCyberCenter

at the MassTech Collaborative

CyberSecureDeck:
Defend the Network!
Card Game

Purpose

A fun way to promote conversation about cybersecurity and ways to identify threats and vulnerabilities, protect vital infrastructure, detect security threats, respond to incidents, and recover from attacks to promote cyber resiliency.

Objectives

- Collaborate and practice cyber incident response actions in a safe, no-fault environment
- Assess what information and resources are needed to respond and recover from an incident
- Identify opportunities to improve cyber incident response plans

Goal: Players in the 8 roles guide the organization through a scenario by helping Identify, Protect, Detect, Respond, and Recover from a cybersecurity incident.

More Scenarios and Injects are available at
MassCyberCenter.org

Directions: ROLES
For the 1-Hour Game: 5+ players
(1 Facilitator, 4+ Players)

- There is one Facilitator, who does not represent a Role in the organization. Their responsibility is to manage the **game play.**
- Facilitator instructions are included in the paper instructions.
- There are 8 Role cards in the game. These 8 Role cards represent all departments within the Organization.
- Each player chooses a Role card. If there are less than 8 players, players should choose more than 1 Role card. All roles must be played.
- Players should immerse themselves in their selected Role, even if they do not perform that function in real life.

MassCyberCenter.org

Role: LEADER

Details:

The **Leader** is the most senior-level position at the Organization. They are responsible for:

- Making strategic, high-level decisions and managing the Organization
- Managing all team members and Roles

As the spokesperson for the Organization, Communications/Media works with the Leader on speech writing and issuing public statements.

The Leader is the **final approver** for any IT actions taken across Organization networks that may disrupt services.

Things to consider in the Leader Role:

- What are the *risks* to the organization if a cybersecurity incident occurs?
- What are the Leader's responsibilities to customers, employees and other constituencies?
- What Roles should be involved in discussions about cyber incidents? Why?

Also Known As: CHAIR – CEO – PRESIDENT – MAYOR – SUPERINTENDENT

Role: COMMUNICATIONS/MEDIA

Details:

Communications/Media is responsible for creating content for all internal and external communications and working with the Leader on writing speeches and issuing public statements.

They also manage the Organization's social media accounts and post content 4 or 5 times per week. To make it easy for the Communications/Media team to access the accounts, they share one complex password.

Things to consider in the Communications/Media Role:

- What Roles should be involved in content creation/communication about a cyber incident?
- What is the Organization's legal responsibility?
- What, if anything, needs to be communicated and to whom?
- How should things be communicated (email, mail, public statement, press, other)?

Also Known As: MARKETING – PUBLIC RELATIONS – COMMUNITY RELATIONS – SPECIAL EVENTS

Role: LEGAL/RISK/COMPLIANCE

Details:

Legal/Risk/Compliance is responsible for writing and reviewing, and interpreting the Organization's policies, contracts and decisions on organizational risk and legal requirements.

Legal/Risk/Compliance also manages the relationship with the cyber insurance company.

Things to consider in the Legal/Risk Compliance Role:

- What is the Organization's legal responsibility in the event of a cyber incident?
- What, if anything, needs to be communicated and to whom?
- When does the Organization notify the cyber insurance company of an incident?

Also Known As: GENERAL COUNSEL – OUTSIDE COUNSEL – GOVERNANCE – RISK MANAGEMENT

Role: OPERATIONS

Details:

Operations is responsible for the Organization's operations, which promote business development, employee productivity and physical safety. Responsibilities include:

- Building Automation Systems (HVAC, elevators, fire systems, etc.)
- Buildings and Property Maintenance including:
  - Access (Physical Security)
  - Landscaping
  - Parking
- Operations is the final approver of all contracts with 3rd-party service providers.

Things to consider in the Operations Role:

- What is the Organization's legal responsibility in the event of a security incident?
- What Roles should be involved in discussions about security incidents? Are they different roles when discussing cybersecurity incidents?
- Which of the Organization's contracts are effected/enforced during a cybersecurity incident?

Also Known As: CHIEF OPERATING OFFICER (COO) – CHIEF OF STAFF – DEPARTMENT OF PUBLIC WORKS (DPW)

Role: FINANCE

Details:

Finance is responsible for all financial transactions inside/outside of the Organization, including:

- Accounts Payable and Receivable
- Payroll
- All quarterly and year-end financial statements including income statements and balance sheets

The payroll system is accessed through a cloud-based portal.

Finance created an organizational policy requiring employees to verify financial account changes before approving financial transactions.

Finance has been given privileged access to sensitive financial files. Only Finance and IT have this access.

Things to consider in the Finance Role:

- What is the Organization's vulnerability to financial loss in the event of a cyber incident?
- What are alternative methods of payment if the payroll system is unavailable?
- Will the organization be able to pay bills/collect revenue?

Also Known As: CHIEF FINANCIAL OFFICER (CFO) – COMPTROLLER – ACCOUNTANT – AUDITOR

Role: INFORMATION TECHNOLOGY (IT)

Details:

The **Information Technology** team is made up of four employees including three employees who manage the network, email and computer provisioning.

There is a Managed Security Service Provider (MSSP) who assists the team with computer and network security.

The email is cloud-based.

Laptops have a standard configuration, and organizational employees all have administrative access to their computers -- allowing them to make changes.

(The head of IT previously advised against employees having administrative access but was overruled by Operations and the Leader.)

Things to consider in the IT Role:

- Do employees know how to report suspicious computer behavior?
- Does the IT team have input in the incident response plan?

Also Known As: CHIEF INFORMATION OFFICER – CHIEF INFORMATION SECURITY OFFICER – APPLICATIONS – DIGITAL TECHNOLOGY

Role: HUMAN RESOURCES (HR)

Details:

HR oversees all personnel decisions in the Organization.

HR in collaboration with other departments also creates:

- Organizational policies, including employment policies, acceptable use policies, and more
- A robust employee benefits package to round out the compensation package

HR reports to the Leader and is the primary contact for employment, disciplinary actions, and promotion decisions.

Things to consider in the HR Role:

As the overseer of all personnel decisions in the Organization, HR sees a lot of "strange pieces" of information that may indicate malicious behavior on the part of employees.

- When does information get escalated to other Roles/departments?
- Who do you notify?

Also Known As: WORKFORCE MANAGEMENT

Role: SECURITY/LAW ENFORCEMENT

Details:

Security/Law Enforcement is responsible for the Organization's physical safety by:

- Investigating all threats related to physical security or employees
- Communicating reportable security incidents to law enforcement or regulatory agencies
- Owns/updates crisis management and incident response plans

The team works closely with Operations to ensure the facilities are secure.

Things to consider in the Security/Law Enforcement Role:

- What is the Organization's legal responsibility in the event of a cyber incident?
- Who would be logical contacts for Security/Law Enforcement to develop prior to an incident?

Also Known As: PUBLIC SAFETY – POLICE – CHIEF SECURITY OFFICER

Directions:
SCENARIOS & INJECTS

How to Use:

15-Minute Discussion: 1 Facilitator, 4+ Players

- Choose 1 Scenario card for the discussion.
- Read the Scenario card to the discussion participants.
- Ask participants, "If this happened at our Organization, what would you do?"
- Use Notes on bottom of Scenario card to help guide discussion.
- Use Hot Wash Card questions for follow-up discussion.

1-Hour Game: 1 Facilitator, 4+ players

- Choose a Scenario card and related Injects.
- Place 8 Role cards, Directions cards, and Org Chart on the table.
- Ask players to choose a Role. All 8 Roles must be played. Have participants take on a second Role if needed.
- Give INJECTS, one-by-one, in numbered order to the Role indicated on the card and ask, "What do you do with this information?"
- Wait for discussion after each Inject.
- After **last** Inject is used, and discussion has ended, read the Scenario to the Organization and go through Hot Wash card questions.

More scenarios and injects are available at
MassCyberCenter.org

Scenario: PHISHING

Details:

Finance receives an email, purportedly from a trusted vendor, asking for a review of an invoice. An employee clicks on the link, causing a malicious file to be downloaded to the Organization's network.

The file remains undetected and is used by hackers to conduct reconnaissance and password stealing for several days before the hackers become operational.

Hackers use administrative privileges to execute their attack and gain access to the building's automation system, phone system, and multiple computers on the network.

Notes

- Can you identify the impacts to customers/employees if this happened?
- Which Roles would be involved in identifying, responding, and recovering from this incident?
- What are some precautions the organization can take to guard against this -- both technical and non-technical?
- Does your organization have a cyber incident response plan that identifies this type of threat and how to respond?

Role: *ORGANIZATION*

Detail:

- Employees begin reporting that the Voice Over Internet Protocol (VOIP) phone system is offline.

_____

What do you do with this information?

_____

MassCyberCenter.org

Role: *OPERATIONS*

Detail:

- Employees from several different Organization locations are calling Operations to say that the HVAC is not working in their location.

- Operations is unable to log into the Building Automation System portal to check temperatures and adjust settings.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Limit OT Connections to Public Internet (2.X)

MassCyberCenter.org

Scenario: PHISHING
Inject 3

Role: *INFORMATION TECHNOLOGY*

Detail:

- The IT team discovers a recent email containing a suspicious URL that was clicked on by an Organization employee.
- This caused several small binary files to be downloaded onto the employee's computer.
- These files created an encrypted connection from the computer to a remote system.
- That connection remained active until the computer was quarantined and removed from the network.
- The file signature of a file found on the computer matches a newly-reported keylogger and ransomware variant.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Email Security (2.M)

MassCyberCenter.org

Role: *LEADER*

Detail:

- The Leader receives a call on their cellphone from a local news reporter asking for a comment on a just-published cybersecurity blog that mentions a Ransomware-for-Hire request targeting the Organization.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Email Security (2.M)

MassCyberCenter.org

Role: *FINANCE*

Detail:

- Suddenly, the Finance team computers stop responding. Shortly thereafter, the computers all display this message:

> We have copied all your sensitive employee and customer records and are prepared to post this information on the internet for all to see unless you pay us $500,000 in Bitcoin by this Friday. That is two days from now.
>
> Tomorrow the price will go up. Time is money.
>
> If you don't believe we have any data, you can contact us and ask for proof.
>
> When you pay us the data will be removed from our disks and we will provide the decryption key.
>
> No decryption Key is publicly available.
>
> You have no other choice if you want your data restored and recovered.
>
> You can trust our word. Contact us here.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Hardware and Software Approval Process (2.Q)

MassCyberCenter.org

Role: *INFORMATION TECHNOLOGY*
Detail:

- The VOIP (Voice Over Internet Protocol) server is displaying a Ransomware notice on its login screen similar to the one observed in Finance.

- The local on-site backup server is displaying a Ransomware notice on its login screen similar to the one observed in Finance.

We have copied all your sensitive employee and customer records and are prepared to post this information on the internet for all to see unless you pay us $500,000 in Bitcoin by this Friday. That is two days from now.

Tomorrow the price will go up. Time is money.

If you don't believe we have any data, you can contact us and ask for proof.

When you pay us the data will be removed from our disks and we will provide the decryption key.

No decryption Key is publicly available. You have no other choice if you want your data restored and recovered.

You can trust our word. Contact us here.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Network Segmentation (2.F)

MassCyberCenter.org

Scenario: PHISHING
Inject 7

Role: *HUMAN RESOURCES*

Detail:

- The HR Director just received an email from a strange email address that claims to be from the Ransomware attacker.

> We have copied all your sensitive employee and customer records and are prepared to post this information on the internet for all to see unless you pay us $500,000 in Bitcoin by this Friday. That is two days from now.
>
> Tomorrow the price will go up. Time is money.
>
> If you don't believe we have any data you can contact us and ask for proof.
>
> When you pay us the data will be removed from our disks and we provide decryption key
>
> Contact us here.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Reporting (4.A)

MassCyberCenter.org

Role: *INFORMATION TECHNOLOGY*

Detail:

- The Managed Services Provider (MSP) supporting your team called and said that it will take about 10 - 14 days to restore all systems from existing backups.

- Upon request, the MSP told you the estimated cost for the MSP to surge overtime to restore all backups within 5 days is $250,000.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Planning and Preparedness (5.A)

MassCyberCenter.org

Role: *COMMUNICATIONS/MEDIA*

Detail:

- Multiple customers are posting on social media that they received an email from hackers stating that their data has been stolen due to the Organization's lax security practices and that they should sue the Organization.
- In an escalated demand, the attackers had said that they would consider not making the customer data public if the customer pays $5 million in Bitcoin.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Reporting (4.A)

MassCyberCenter.org

Scenario: PHISHING
Inject 10

Role: *SECURITY/LAW ENFORCEMENT*

Detail:

- You receive a call from a Law Enforcement partner
  1. Asking if you need help, and
  2. Providing a friendly reminder about State Data Breach Notification Laws

---

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Reporting (4.A)

MassCyberCenter.org

Scenario: PHISHING
Inject 11

Role: *INFORMATION TECHNOLOGY*

Detail:

- The Incident Responder's forensic review revealed the following information:
  - Finance received an email, purportedly from a trusted vendor, asking for a review of an invoice. An employee clicked on the link, causing a malicious file to be downloaded to the Organization's network.
  - The file remained undetected and was used by hackers to conduct reconnaissance and password stealing for several days before the hackers became operational.
  - Hackers used administrative privileges to execute their attack and gain access to the building automation system, phone system, and multiple computers on the network.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Log Collection (2.T)

MassCyberCenter.org

Scenario: PHISHING
Inject 12

Role: *LEADER*

Detail:

- The Leader asks the team to convene for a meeting to discuss several items:
  - What is the business impact of this cybersecurity incident?
  - What are the best options? Backups? Pay ransom?
  - Who do we notify? When?
  - What are the projections for service disruptions?

CISA Cybersecurity Performance Goal:
Incident Planning and Preparedness (5.A)

MassCyberCenter.org

Scenario: SOCIAL ENGINEERING

Details:

A member of the Operations team goes on vacation to the Caribbean for a well-deserved two-week vacation.

When the employee returns, she discovers that while she was out, someone contacted HR via her work email to change her banking information.

HR changed the banking information, and the employee's last paycheck was not deposited into her account.

Notes:

- What can the organization do to report this and try to recover the funds?
- Which Roles would be involved in identifying, responding, and recovering from this incident?
- What are some precautions the organization can take to guard against this -- both technical and non-technical?
- Do you have a cyber incident response plan that identifies this type of threat and how to respond to it?

Scenario: MALWARE

Details:

A new employee in Human Resources reported that their desktop computer was "acting funny." When the IT Department does some troubleshooting, they discover malware on the employee's computer.

When IT talks to the employee about how the malware may have been introduced onto the computer, the employee was unsure. The employee did mention that they found a "beat-up" old thumb drive in the parking lot they thought might be good to transport files; so, they plugged it into their computer's USB port. IT concluded that the thumb drive was the most likely source of the malware and was inadvertently introduced by the employee.

Notes:

- What are some precautions you can take to guard against malware being introduced into company devices and networks?

- Which policies should include guidance on employee use of thumb drives?

- As the thumb drive originated in the parking lot, what are some investigative steps the company can take to determine who dropped it?

- Which roles should be involved in discussing this issue?

Details:

An employee from the Communications department reported that their computer was not opening files and "strange things" were happening. When the IT Department did some troubleshooting, they discovered malware on the employee's computer. The employee was unsure how the malware got on the computer, but mentioned that they had installed a new video game app. IT concluded that the malware was introduced onto the computer when the app was downloaded.

Notes:

- What are some precautions your organization can take to safeguard company devices and networks?
- Which policies should include guidance on employee use of unauthorized software and applications?
- Does the organization have an approved hardware and software list?
- Does your organization send reminders to all employees about acceptable use of hardware and software?
- Which roles should be involved in discussing this issue?

Scenario: BUSINESS CONTINUITY

Details:

It's a busy summer Tuesday at the Organization and Massboro Road & Paving is repaving the parking lot.

Suddenly employees cannot access the internet. This impacts all business operations: communications, finance, and more. What is going on?

IT troubleshoots the situation and finds that they cannot reinstate internet access as it appears that the paving company has inadvertently severed both the primary and fail-over internet connections for the organization while paving the lot.

Notes:

- Is there a business continuity team and plan?
- Which roles should be involved in discussing this issue?
- Are there immediate actions to take to protect data?
- How would the organization remediate the situation and get back to business?
- How do you communicate the outage, and what do you say:
  - To employees/third parties/customers?

Scenario: INSIDER THREAT

Details:

A member of the Operations team has been making negative comments about Organization employees, as well as negative statements about a product currently being developed.

The employee's manager has given the employee feedback about negative comments concerning products and other employees in the past and counseled them not to make such comments.

The most recent comment made by the employee, as reported by another member of the Operations team, was, "If it was up to me, I would never let this product make it to market."

Notes:

- Does your organization have an Insider Threat Policy?
- Which Roles would be involved in discussing this situation?
- What characteristics should be considered as part of an "insider threat?" (Access to information, attitude/intent, performance, technical activity, criminal intent, and more.)

Directions:
POST EXERCISE HOT WASH

Instructions:

Use this card after the 15-Minute Discussions, or when all Inject Cards are used up during the 1-Hour Game.

- Share the Scenario information.
- Ask the group questions about the game to facilitate discussion :
  - What is happening within the Organization?
  - What steps is each Role taking to respond to the events? How about other Roles?
  - Information flow: How should all this information come together?
  - What communications are important during an event like this, and when?
  - Who would you prioritize communications with (internally/externally)?
  - Do you consider activating a Cyber Incident Response Plan (CIRP)? Why?
  - What elements would you consider to be part of a CIRP?
  - How did the game go? What would you do differently?

Thank you for playing!

For more scenarios, injects and resources, please visit **MassCyberCenter.org**

MassCyberCenter wishes to thank The Commonwealth Fusion Center and the Cyber Resilient Massachusetts Working Group for their support in developing this game.

MassCyberCenter
at the MassTech Collaborative