Conducting an online Breach Response Tabletop Exercise

TEAM CISO

Wednesday April 8th 12-1pm EST

https://teamciso.com/breach-response-webinar

Agenda

Creating a Breach Response Plan

Selecting the Cyber Security Incident Response Team (CSIRT)

Understanding the phases of a Breach Response

Developing Operational "Playbooks"

Who are your Stakeholders?

Communications

- **Reporting a Breach**
- **Creating Communications Templates**
- **Who can speak for your business?**
- **Managing Social Media**
- **How communication is much is too much?**

Planning for your Tabletop Exercise

Developing CyberSecurity Scenarios to test

Iterating from "Lessons Learned"

Who is TeamCISO?

Founded in 2015, TeamCISO is a Toronto based Cyber Security company with the mission of bringing Enterprise security practices to Small and Medium Businesses.

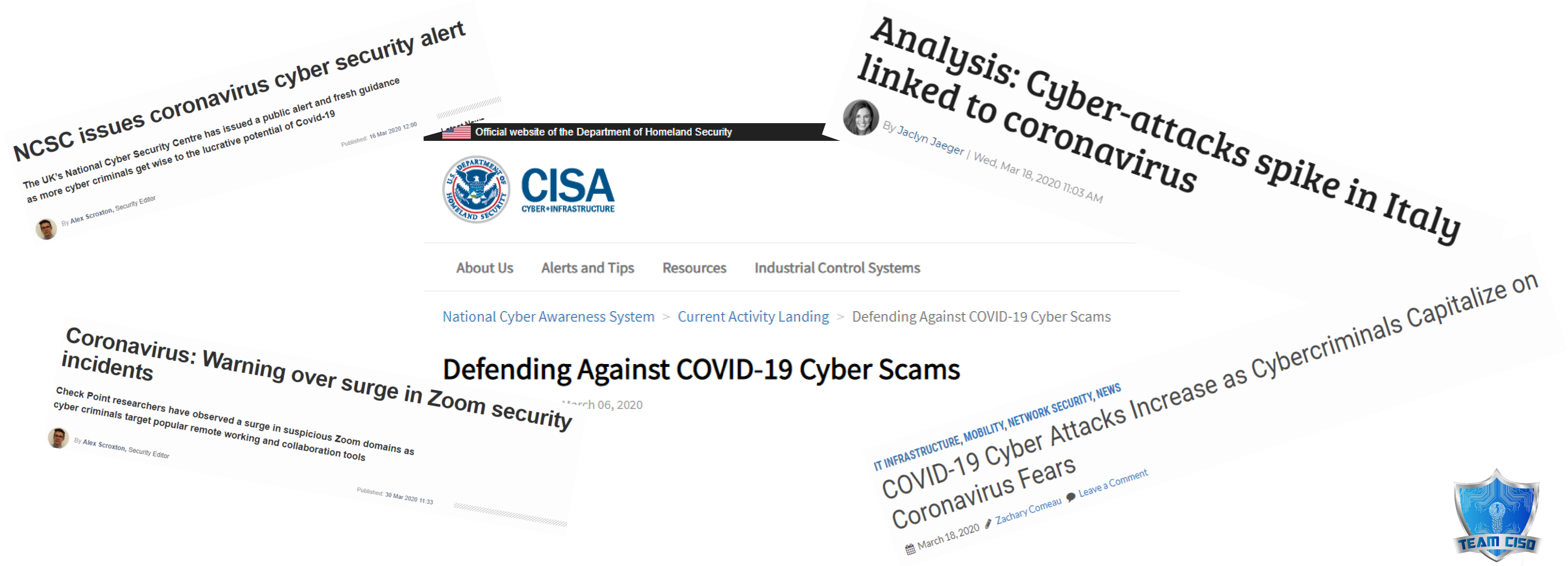
We provide Cyber Security Governance and Operational assistance across Canada.

From Virtual, Interim, or Advisory CISO, to penetration testing and vulnerability assessments, we are your holistic Cyber Security Partner.

info@teamciso.com

https://teamciso.com

The best time to plan for a crisis is: Before the crisis…



NCSC issues coronavirus cyber security alert

The UK's National Cyber Security Centre has issued a public alert and fresh guidance as more cyber criminals get wise to the lucrative potential of Covid-19

By Alex Scroxton, Security Editor

Published: 16 Mar 2020 12:00

Official website of the Department of Homeland Security

CISA CYBER+INFRASTRUCTURE

About Us Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity Landing > Defending Against COVID-19 Cyber Scams

Defending Against COVID-19 Cyber Scams

March 06, 2020

Analysis: Cyber-attacks spike in Italy linked to coronavirus

By Jaclyn Jaeger | Wed, Mar 18, 2020 11:03 AM

Coronavirus: Warning over surge in Zoom security incidents

Check Point researchers have observed a surge in suspicious Zoom domains as cyber criminals target popular remote working and collaboration tools

By Alex Scroxton, Security Editor

Published: 30 Mar 2020 11:33

IT INFRASTRUCTURE, MOBILITY, NETWORK SECURITY, NEWS

COVID-19 Cyber Attacks Increase as Cybercriminals Capitalize on Coronavirus Fears

March 18, 2020 Zachary Comeau Leave a Comment

Breach Notification Legislation: Canada

PIPEDA November 2018 Office of the Privacy Commissioner

The law requires that you report any breach of security safeguards involving personal information under your control if it is reasonable in the circumstances to believe that the breach of security safeguards creates a real risk of significant harm (RROSH) to an individual.

https://www.priv.gc.ca

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm include the sensitivity of the personal information involved in the breach of security safeguards and the probability the personal information has been/is/will be misused.

HIPAA and PCI have even more stringent requirements when it comes to Healthcare or Payment Card Information.

Breach Notification Legislation: US

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

https://www.ncsl.org

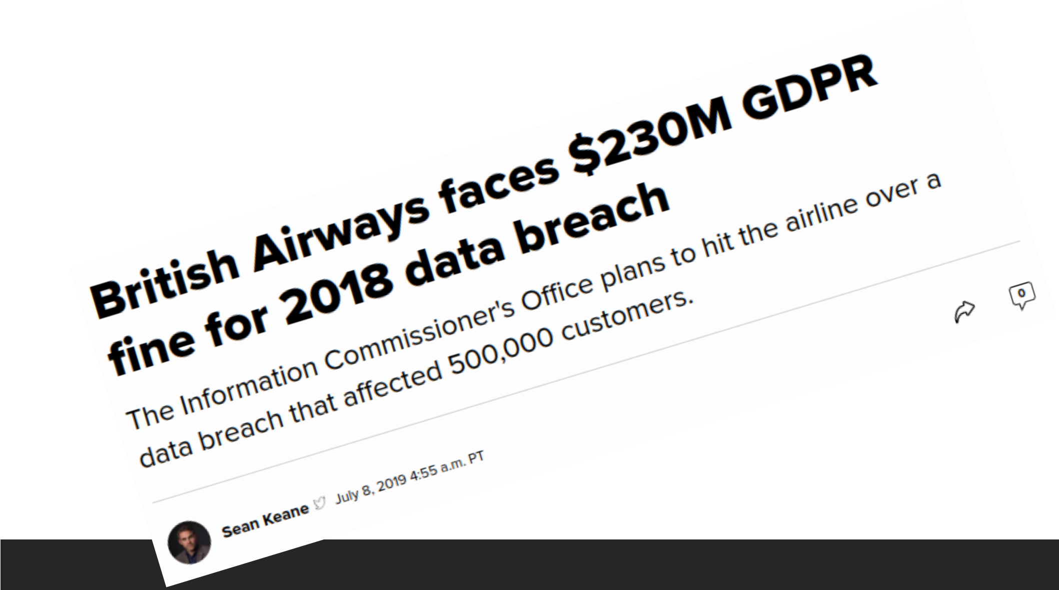
California and New York State have the most stringent Breach Notification Requirements

Breach Notification Legislation: EUROPE

The European Union General Data Protection Regulation (GDPR) is by far the most precice and stringent among the published Breach Legislations.

Violators of GDPR may be fined up to €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater.

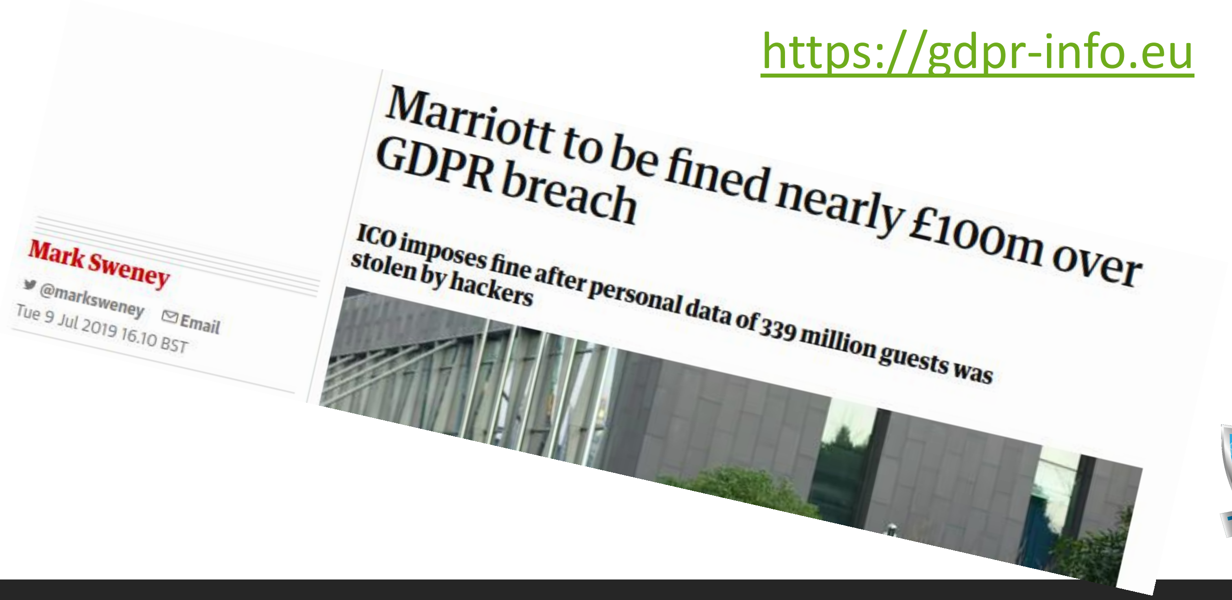
https://gdpr-info.eu



British Airways faces $230M GDPR fine for 2018 data breach

The Information Commissioner's Office plans to hit the airline over a data breach that affected 500,000 customers.

Sean Keane July 8, 2019 4:55 a.m. PT



Marriott to be fined nearly £100m over GDPR breach

ICO imposes fine after personal data of 339 million guests was stolen by hackers

Mark Sweney

@marksweney Email

Tue 9 Jul 2019 16.10 BST

Creating a Breach Response Plan

Purpose

A breach response plan provides a detailed roadmap to follow when a breach is discovered. It is the process by which a breach is evaluated, communicated, contained, eradicated, and recovered from.

Elements of a Response Plan

To be effective, a breach response plan should include the following:

- A definition of a breach
- A list of response team members
- The action steps for handling the breach
- Communications templates for stakeholders
- A follow-up procedure

Incident vs Breach: What's the difference?

A breach always starts with a cyber security incident:

HIPAA defines security incidents as attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

It becomes a "Breach" when the incident is successful in disclosing, modifying, or destroying the information.

It becomes a "reportable breach" when the information disclosed, modified, or destroyed is of a nature to cause harm to an individual or company.

Selecting the Cyber Security Incident Response Team (CSIRT)

The **Cyber Security Incident Response Team** needs to be selected early in the process.

It should be a mix of Accountable Executive with the authority to make decisions and technical staff with the skills and ability to identify, contain, eradicate, and recover from a series of potential breach scenarios.

Suggested Cyber Security Incident Response Team Members

Executive:

CEO / President

CIO / IT Manager

Human Resources

Corporate Comms

Legal

Privacy

Technical Analysts:

Network

Voice

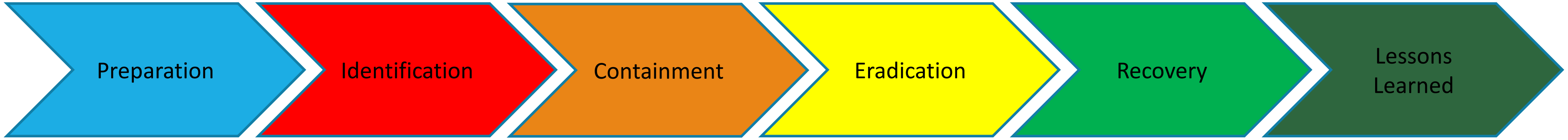
Servers

Cloud

Desktop

Other?

Understanding the phases of a Breach Response



Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned

Incident and Breach response processes have been worked out over the past several decades. The above phases have been globally adopted as appropriate.

Developing Operational "Playbooks"

Preparation:

In the preparation phase, you would develop Policies, Standards, and Procedures for the management of each and every piece of technology used within your organization.

Document security controls and configurations for authentication/authorization, encryption, backup, transfer, etc…

Document you Incident Response Team and their Roles and Responsibilities

Create your Security Operations Center (In-house or 3rd party MDR)

Train entire team on incident response procedures

https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1559689083.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Playbooks : Detection

You cannot properly identify a security incident or breach without appropriate detection tools in place.

- Perimeter controls (Firewalls, Proxies, Gateways, VPN, IDS/IPS)
- Endpoint Monitoring (Laptop, Desktop, Mobile, Server)
- Network Traffic (wired and Wireless)
- Server logs
- External Threat Intelligence

- Look for known suspicious activity (SIEM, low hanging fruit)
- Look for Anomalous behavior (Threat hunting)
- Raise alerts on anything suspicious

Playbooks: Components

Flowcharts vs Checklists

- Flowchart are good for decisions that lead to multiple paths
- Checklist are good for monolithic lists of steps

Create RACI charts

- Identify WHO is Responsible / Accountable / Consulted / Informed

Contact List

- Have contact info in playbook
- Have backups where possible

Developing Operational "Playbooks"

Identification:

Not every “event” or “alert” will be an incident.

Not every incident will be a breach.

Not every breach will require reporting.

- What happened to cause the alert? (Malware, fat fingering Admin, Excessive Privileges, failed hardware/software, Phishing Attack, Hacker, etc…)
- What data was compromised?
  - What is Personally Identifiable Information (PII)?
  - Was it Healthcare Information?
  - Was it Payment Card Information?
  - Was it Corporate Intellectual Property (Crown Jewels)?
- What is the magnitude of the breach?
- Could its disclosure cause potential harm to a person or company?

Developing Operational "Playbooks"

Containment:

What controls do you have in place to stop the spread or exfiltration of the incident?

- Perimeter controls (Firewalls, Proxies, Gateways, VPN, IDS/IPS)
- Internal network controls (VLAN Segregation, zoning, routers etc..)

Eradication:

What controls do you have in place to stop the spread or exfiltration of the incident?

- Remove malware or rebuild systems
- Remove back doors, delete accounts, change passwords, etc…

Developing Operational "Playbooks"

Recovery:

- Harden systems
- Implement new controls
- Bring systems back online

Post Mortem:

What did we learn from *this* incident?

- Update policies and procedures
- Update Cyber Scenario Playbooks
- Implement new controls if required

Who are your Stakeholders?

In the case of a reportable breach, your first stakeholder would of course be those who have received harm.

External:

- Privacy Commissioner
- Law Enforcement
- Press
- Business partners/vendors
- Customers

Internal:

- Executive Committee
- Board of Directors
- Employees

Communications

As part of your Planning, you will have selected a spokesperson to represent your communications.

In a larger org, this would typically be your Corporate Communications department, with Legal, Privacy, and Human Resources as advisors.

In the chaos of crisis, there is no time to clearly think through and articulate the message you wish to deliver to each type of stakeholder, internal and external. Understand that while the overall message may be the same, the level and type of detail as well as purpose may differ.

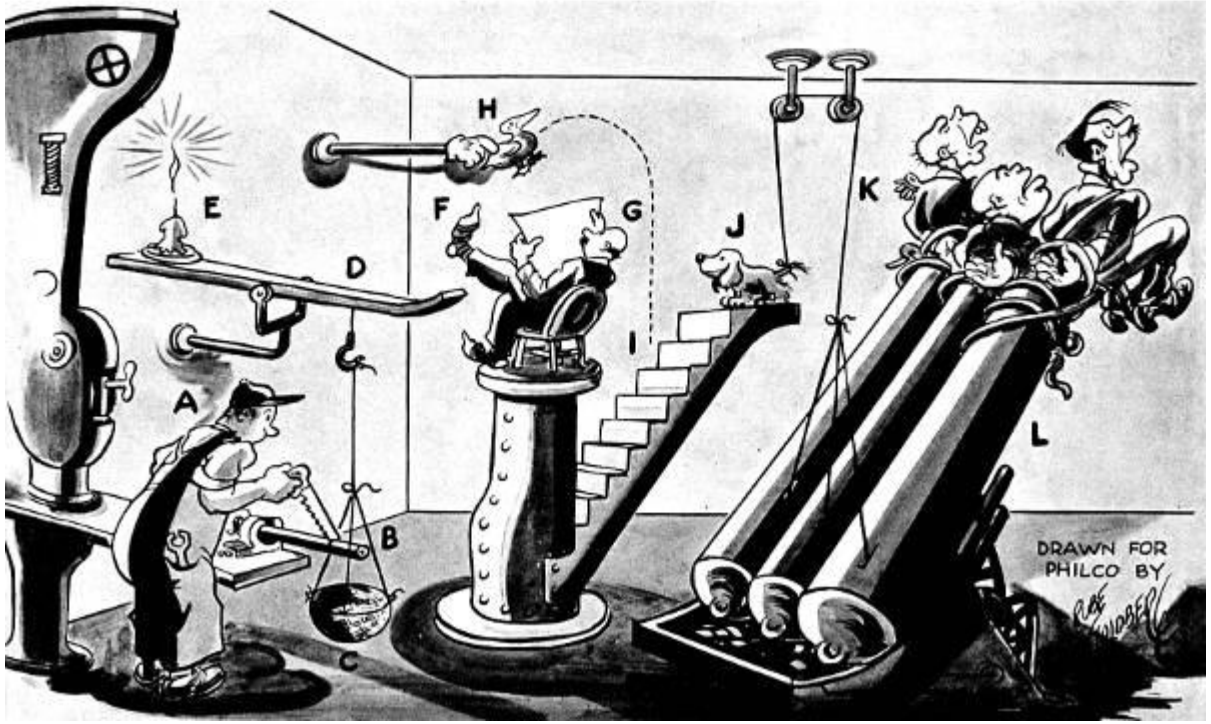
Remember that while you are doing you due diligence to report the breach, you also need to manage brand and reputation.

Communications

Timing is everything.

- Start with trusted internal and key stakeholders first.
- Make sure that as part of the internal messaging, your employees are aware that *they* are not at liberty to disclose details even - “off the record” - but are to refer to the spokesperson.
- Expect that at least one person will (intentionally or inadvertently) communicate the internal message externally shortly after the communication goes out.
- Always prepare written statements for the media in advance.
- Don’t be afraid to engage a professional Public Relations firm.

Testing your Plan…



Planning for your Tabletop Exercise

A “Tabletop Exercise” is an idea taken from Disaster Crisis Management

Once all the preparation, documentation, and training have taken place, gather together the members of the Cyber Security Incident Response team to validate that the plans and training are sound, and that no steps have been forgotten.

Typically this is conducted off site over the course of a half day or so, walking through several known Cyber Security Scenarios.

Developing Cyber Security Scenarios to test your planning

Pick three to four realistic *current* Cyber Security scenarios to work through.

Make sure each scenario has a clear objective:

- Problem solving
- Ability to determine risk
- Communications
- Delegation
- Identify weaknesses in procedures

Some good examples here:

https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/

https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Developing Cyber Security Scenarios to test

Threat Actors:

Natural Disaster

Ignorant user

Malicious Insider

Hacker

Potential Scenarios:

Rampant Virus

Network Denial of Service

Spear Phishing

Privileged Credentials found in Cloud Storage

Iterating from "Lessons Learned"

Tabletop Exercises are designed to stress test both your team’s ability to work together and communicate efficiently under duress.

Chaos is king.

Are your playbooks valid?

Did you miss any steps?

Was everybody engaged and doing their part?

What did we miss?

Virtual War Room

Cyber Security Events don’t wait for timing to be convenient.

Now is as good a time as any to start

These are all practices that can be developed, documented, and tested remotely!

Online products like Microsoft Teams, Twitch, Slack, Webex and Zoom are all viable products to help you quickly pull together your CSIRT and manage communications.

Thank you.

And a Shameless Plug…

Breach The Keep

https://breachthekeep.com

A Breach Response Tabletop preparedness exercise for corporate executives.

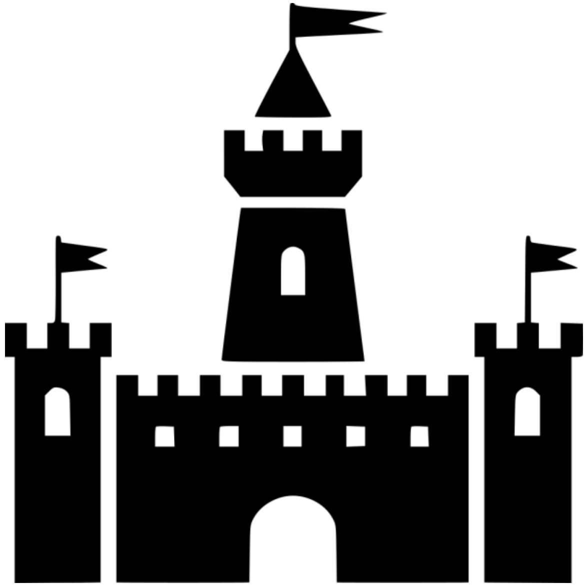
It is an exciting team building Cyber Security experience for problem solving during a breach or ransomware event.

GET BREACHED!

info@breachthekeep.com

CYBERSECURITY TABLETOP EXERCISE
BREACH THE KEEP
TEAM CISO
siberX
DURHAM COLLEGE
TEAM BUILDINGCOLLABORATIONIMPROVED COMMUNICATIONLEADERSHIPTEAM WORK
IS YOUR TECHNICAL INCIDENT RESPONSE AND
EXECUTIVE CRISIS MANAGEMENT PREPARED?

Breach The Keep



We will take you back in time into the realms of medieval and have a little fun with our version of Dungeons and Dragons.

Through multiple scenarios we can help enhance your company's team building abilities, identify gaps within the team and improve real world incident response.

Bringing you onsite scenario roleplay , let us take you into a world of excited learning, improving your cybersecurity responses, isolating cyber threats and much more in one of the available tracks: technical incident response and executive crisis management.

To book an experience send a request to info@breachthekeep.com

Michael Ball, vCISO at TeamCISO Inc.

CyberSecurity Adviser and founder of TeamCISO with over 25 years in Infosec.

Currently developing the "Virtual CISO" practice for small to mid-tier businesses, and occupying the role of Virtual CISO in several Canadian Mid-Market organizations. Over the past 15 years Michael has helped create the Office of the CISO in two large global Insurance Companies.

Michael is a regular speaker/panelist at CyberSecurity conferences across North America, and provides onsite CyberSecurity guidance across many business verticals.

Michael.ball@teamciso.com

https://teamciso.com