Cyber Incident Response Planning

Are You Prepared?

Secure Data Consulting Services

Trends & Statistics 2022

- ✓ NJ receives 10 million cyber attacks per day.
- ✓ Cybercriminals can penetrate 93% of company networks.
- ✓ Cyber attacks on the education sector up by 75%.
- ✓ Cyber attacks on the government sector up by 47%.
- ✓ 43% of cyber attacks are aimed at small business.
- ✓ The United States remains the most highly targeted country with 46% of global cyberattacks directed towards Americans.

Secure Data Consulting Services

Preparedness Is Key for Cybersecurity Incident Response

- ✓ The JIF has provided a Cyber Incident Response template.
- ✓ Review your Incident Response Plan and Business Continuity Plan with your IT professional.
- ✓ Do a yearly tabletop exercise.
- ✓ Take a step-by-step approach.

Secure Data Consulting Services

Organization

Step 1

- ✓ Determine who has overall responsibility for the plan, then broaden that thinking to create the extended team — think IT, legal, finance and HR.
- ✓ Specify the roles and responsibilities of each member of the incident response team.
- ✓ The plan should include contact information for each team member.

Preparation/ Protection

Step 2

- ✓ Prioritize all systems that must be kept online or brought back online first and set up policies to protect them.
- ✓ Next, ensure that relevant security tools such as firewalls, anti-virus, vulnerability scans and patching systems are in place and kept up to date.
- ✓ Identify gaps in security and create a remediation plan. Ensure backups are stored offline and recovery is tested periodically.

Preparation/ Protection

Step 2 - continued

- ✓ Provide security awareness training to employees and elected leaders, and even to citizens if possible.
- ✓ Create a detailed list of instructions for handling incidents.
- ✓ Test all of this periodically with the IR team.

Detection and Analysis

Step 3

- ✓ When an incident is detected, the process tree should be activated so team members can spring into action. This phase includes determining the cause and impact of the incident.
- ✓ If it is severe or catastrophic, information needs to be gathered for further analysis and reporting to relevant authorities.
- ✓ The plan should include information about mandatory reporting, as well as protocols for notifying local and state law enforcement, including Homeland Security and the FBI, if needed.

Containment and Recovery

Step 4

- ✓ This phase involves taking action to control the attack and limit the damage and impact. It may involve eradicating malware, mitigating misconfigurations or identifying other hosts that might be infected, so information on how to respond to each type of incident is included here.

Containment and Recovery

Step 4 - continued

- ✓ This section of the plan also includes steps necessary to restore the affected systems to normal operation, which might involve restoring from backups, rebuilding from a secure baseline, replacing compromised files with clean versions, patching or changing passwords.
- ✓ Once the incident has been resolved, the plan includes a step for evaluating lessons learned and incorporating that information into a revised IR plan.

Have a Roadmap Available

CYBER INCIDENT ROADMAP

You expect or know of a cyber incident.
The clock is ticking to avoid further damage to you and your stakeholders.

Step 1: Report to Joe Lisciandri at Qual-Lynx by calling (609) 601-3191

Step 2: Call XL Catlin 24/7 Breach Hotline at (855) 566-4724 for triage.
BURLCO JIF Policy #: MTP003948305

- XL Catlin Cyber Claims Specialist steps in to manage the claim for you
- When needed, your Cyber Claims Specialist will engage an XL preapproved expert cyber attorney
- In addition to their duties, the attorney will engage any other needed experts

Your Cyber Claims Team will walk you through every step of responding to the incident and offer assistance and take actions on your behalf as necessary.

Burlington County Municipal Joint Insurance Fund
Established in 1991
South Jersey Communities Securing Their Future

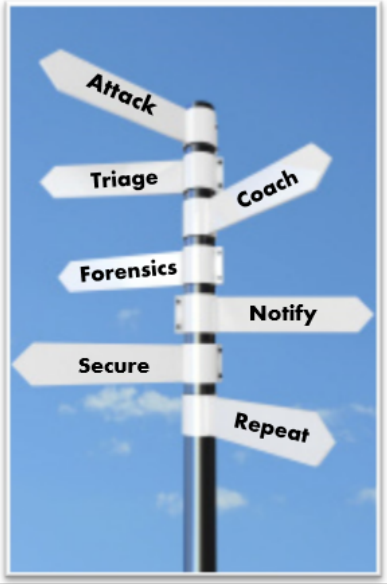
Other Considerations

XL Catlin online cyber portal:
www.cyberriskconnect.com
Access Code: 10448

Claims Administrator: Qual-Lynx
(609) 601-3191

Fund Attorney: David DeWeese
(609) 522-5599

MEL Coverage Bulletin 18-25



Test the Plan

Take time to test and exercise your Incident Response Plan and your Business Continuity Plan.

Revise and update accordingly.

Incident Response Plan and your Business Continuity Plan go hand in hand.

Secure Data Consulting Services