The Cyber Resilient CFO

Key Takeaways from the Panel Discussion

October 6, 2021

CFO FORUM

AON
Empower Results®

STROZ FRIEDBERG
an Aon company

Key Takeways

- Ransomware Readiness
- Disaster Recovery Planning
- Cyber Insurers focus on Key Controls
- Incident Response Preparation and Call Tree

Ransomware Readiness

- Current Trends within the Ransomware Industry

  – The new trend in Ransomware not only encrypts the enterprise's data and shuts down operations but exfiltrates the data as well.

  – The exfiltrated data is then used for extortion if the enterprise does not pay the ransom. The bad actors threaten to post the data on the dark web or public facing websites.

  – Ransomware groups are going "Corporate"
    - Now a billion-dollar industry
    - Gravitating towards joint partnerships, profit sharing, playbooks, and IP sharing
    - Allows the criminal groups greater speed, access, and repeatable processes
    - The Ransomware demands have increased
    - 80% of attackers have the ability to exfiltrate data

- **Damages to businesses and organizations are expected to be $20 billion in 2021[2]**
- **Global ransomware reports are up more than 715% from 2019 to 2020[3]**
- **Ransomware payments have increased 60% in value since 2019[4]**

Ransomware Readiness

- Ten Critical Steps to Prevent and Detect Ransomware

1. **Phishing Awareness Training**, to educate employees and end-users on how to spot phishing emails and know the red flags to drive down clicks on the malicious emails many ransomware attackers use to gain a foothold in a network.

2. **Disabling Accessibility of Remote Desktop Directly from the Internet**, to prevent ransomware attackers from brute-forcing Internet-facing RDP services to gain entry into a network.

3. **Properly Configured URL Filtering and E-mail Attachment Sandboxing**, to prevent malware contained in ransomware emails from executing or going unnoticed.

4. **An Advanced Endpoint Detection and Response ("EDR") Solution**, to detect and potentially quarantine ransomware and other advanced malware, and also to facilitate enterprise forensics in the event of an attack.

5. **An Advanced Malware Detection Tool that Inspects Network Traffic**, to identify ransomware and other malicious packets or network traffic flowing over the wire.

6. **16+ Character Service Account and Domain Admin Passwords**, to prevent ransomware and other hackers from cracking weak admin user names and passwords. Optimally, these strong passwords should be rotated regularly, using a Privileged Access Management (PAM) tool. Ransomware attackers use these cracked credentials to move laterally and deploy their ransomware.

7. **Lateral Movement Detection Tools.** After gaining a foothold, ransomware actors typically move laterally using compromised IT credentials. Detecting that anomalous lateral movement normally enables the attack be shut down before ransomware is deployed.

8. **A Properly Configured Security Information and Event Management ("SIEM") Platform** that aggregates event, security, firewall and other logs. Trying to respond to and recover from a ransomware attack without a SIEM is very difficult, as visibility through local, non-centralized logs is often poor.

9. **A Continuous Security Monitoring Function**, which provides continuous monitoring and threat hunting using collected logs and alerts.

10. **Locking Down Software Deployment and Remote Access Tools** (such as SCCM, PDQ, and PsExec) to a small set of privileged accounts with multi-factor authentication where possible. Once they have secured elevated privileges, ransomware attackers typically commandeer SCCM/PDQ/PsExec accounts to push the ransomware executable across the network.

Disaster Recovery Planning Guidelines

IT DR Plan Overview

- IT DR goals and objectives
- IT DR Scope
  - what systems/data centers etc
- IT DR Definitions
  - within the plan
- Recovery Tiers and Dependencies
- IT DR Roles and Responsibilities
  - who does what
- DR Plan summary

IT Infrastructure Overview

- Data Center, Third party locations, Cloud (what/where)
- IT Core Services
- Storage
- Compute
- Applications/databases
- IT Service Desk

IT DR Plan Phases

- Impact assessment procedures
  - what is the damage?
- Declaration and plan activation
  - who makes the decision with what criteria?
- Technical recovery procedures
- Recovery validation
  - sync data, everything work as expected?
- Failback procedures

IT DR Plan Procedures

- IT DR Communications process (internal/external)
- IT DR Operations considerations
- IT DR Escalation procedures
- IT DR Validation
- IT DR Failback procedures
- IT DR Security Considerations
- IT DR Post Mortem/Lessons learned
- IT DR Plan Tabletops and Exercises
- IT DR Plan access and maintenance

Cyber Insurance—Nine Key Control Areas

- Ransomware Supplemental Addendum started January 2021 in addition to the standard Cyber form
- More technically detailed questions
- Rigorous underwriting
- Companies need to have positive responses for ALL key areas of focus

Multi-factor Authentication (MFA)	Endpoint Protection & Response (EDR)	Phishing Exercise/ Cyber Awareness Training
Patch Management	Secure RDP/VPN	Incident Response Plan
Active Directory/Service Accounts	Disaster Recovery/Backups	Email Filtering

Incident Response – Don't pick your team on the day of the game

Best Practices for Developing your IR Team

Choose the partners you would like to work with prior to any event. In time critical situations, there should be a comfort level that due diligence has been completed to ensure the right team has been vetted and assembled. This includes:

- Incident Response Provider (often 2)
- Outside Counsel/Breach Coach
- Notification and Post Breach Services
- Public Relations
- eDiscovery team
- Investigations Group
- Any other partner related to the nature of your business and operations

How to pick your IR team

Other Considerations

- Your cyber policy carrier will have a pre-approved panel of multiple skillset providers if a breach or incident occurs. You can proactively contact the providers and determine who is the best fit to work with in the event of an incident

- Notify your carrier and make them aware of your preferred partners in the different skillset areas. If you have a preferred partner who is not on the panel you can request they be added for your preferred partners

- Contracts and other legal matters: gather the necessary contracts upfront and vet them through your organization's legal team to avoid redlines and edits during a critical timeframe

- Identify your key Internal Stakeholders such as your General Counsel, Risk Management Team, Compliance Team, Information Technology Team(s), Cyber Security Team, C level, Individual Business Unit leaders, Public Relations, Marketing

Call Tree Example

Develop a Call Tree to implement in the event of a cyber incident, event, or breach

- Contact your insurance broker or Aon Support team as soon as possible to help coordinate resources.
- Notify the “Carrier” Cyber Breach team that you may have an incident and that you have an Incident Response retainer and/or prefer to use Stroz Friedberg or other Forensic firm as your Incident Response provider.
- Contact your Forensic Incident Response Team (Stroz Friedberg – 404-822-5909, or other provider)
- Contact your Outside Counsel, PR firm, Data notification firm, etc.
- Inform internal stakeholders in Finance, Legal, IT and Operations

IR Action Items

- Log Retention – review how long your logs are kept (server, storage, end user devices, firewalls, etc.). The logs are key to preserving “digital breadcrumbs” during an investigation. The longer the retention period the better (rule of thumb)

- Preserve digital evidence. Do not reimage or wipe compromised servers, desktops, or laptops. Take them offline immediately.

- Develop a formal Incident Response Playbook that includes all aspects of your organization.

- Practice the Incident Response Playbook via a Tabletop simulation of a breach with all stakeholders

- Don’t go it alone. The threat landscape is constantly changing, partner with expertise that practices incidents on a daily basis

- Asset Management – Identify the enterprise’s most valuable digital assets and safeguard their protection. Use “least privilege access” method to determine who has access to the data and why

- **END USER AWARENESS AND TRAINING:** The majority of incidents begin with a phishing exercise that are avoidable through via **ONGOING** end user awareness and training (phishing/social engineering exercises)

Questions? Contact us

Kristin Adams
Executive Vice President
t + 404.264.3020 | m + 917.543.9125
Kristin.Rambo.Adams@aon.com

Aaron Bartlone
Vice President of Cyber Solution Enterprise Sales
+1.440.610.3613
Aaron.Bartlone@aon.com