May 9, 2024

Maturing the Plan: Developing the Infrastructure for Efficient Cyber Incident Response

Elizabeth (Liz) Dill, Partner, Co-Chair Advisory Compliance Practice
Mullen Coughlin, LLC

Matt Ahrens, Vice President, Forensic Services Practice
Charles River Associates (CRA)

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Elizabeth (Liz) R. Dill

Partner & Co-Chair, Advisory Compliance
Mullen Coughlin LLC

Matt Ahrens

VP, Forensic Services
Charles River Associates (CRA)

Overview

A **Cyber Incident Response Plan** (IRP) serves as the basis for an organization's incident response procedures. Equally crucial for a successful response is having the necessary infrastructure to support the outlined procedures, ensuring that the IRP is feasible, attainable and customized to fit the organization's technological and operational capabilities and infrastructure.

In this session, we will explore the typical deficiencies in organizations' incident response infrastructure, as seen from the viewpoints of breach counsel and digital forensics investigators. We will also discuss proactive steps to address these gaps and strengthen the process for a more efficient and effective incident response.

Privacy+ Security Forum

Why It's Important – Incident Statistics

Privacy+ Security Forum

2021

Incident Type	Count
Ransomware	1,153
Business Email Compromise (BEC) – Total	1,059
BEC – Other	698
BEC – Wire Fraud	361
Third-Party Breach	623
Network Intrusion	559
Other	367
Inadvertent Disclosure	209
Total	**3,970**

2022

Incident Type	Count
Business Email Compromise (BEC) – Total	1,077
BEC – Other	733
BEC – Wire Fraud	344
Ransomware	732
Network Intrusion	382
Third-Party Breach	316
Other	245
Inadvertent Disclosure	207
Total	**2,959**

2023

Incident Type	Count
Business Email Compromise (BEC) – Total	1,343
BEC – Other	996
BEC – Wire Fraud	347
Ransomware	884
Third-Party Breach	749
Other	403
Network Intrusion	323
Inadvertent Disclosure	218
Total	**3,920**

2024 (through April)

Incident Type	Count
Business Email Compromise (BEC) – Total	481
BEC – Other	353
BEC – Wire Fraud	128
Ransomware	318
Vendor Breach	301
Other	125
Network Intrusion	108
Inadvertent Disclosure	79
Total	**1,412**

Why It's Important – Incident Statistics

Privacy+ Security Forum

2021

Industry Sector	Count
Professional Services	1,024
Manufacturing and Distribution	704
Healthcare and Life Sciences	520
Financial Services	461
Technology	372
Education	215
Non-Profit	205
Government	200
Hospitality and Entertainment	152
Retail/e-Commerce	73
Energy	37
Total	**3,970**

2022

Industry Sector	Count
Professional Services	773
Manufacturing and Distribution	448
Healthcare and Life Sciences	376
Financial Services	350
Technology	333
Non-Profit	157
Education	142
Hospitality and Entertainment	139
Government	122
Retail/e-Commerce	84
Energy	34
Total	**2,959**

2023

Industry Sector	Count
Professional Services	928
Financial Services	588
Healthcare and Life Sciences	572
Manufacturing and Distribution	538
Technology	372
Education	245
Non-Profit	208
Hospitality and Entertainment	169
Government	138
Retail/e-Commerce	130
Energy	32
Total	**3,920**

2024 (through Q1)

Industry Sector	Count
Professional Services	372
Healthcare and Life Sciences	266
Manufacturing and Distribution	176
Financial Services	159
Technology	114
Education	79
Hospitality and Entertainment	66
Government	59
Non-Profit	59
Retail/e-Commerce	39
Energy	23
Total	**1,412**

Why It's Important – Legal Landscape

Privacy+ Security Forum

- **Growing number of laws and regulations requiring notification for data breaches**, some target specific industries (*e.g.*, public companies, healthcare), some concern specific data elements, and definitions may overlap or be inconsistent
- **Similarly, a growing number of law requiring** organizations to have incident response plans that are current and are accurately reflective of their practices
- **Increasing regulatory activity**, including more active authorities, more detailed requests for information, and increased enforcement
- **Courts imposing divergent standards for plaintiffs** to bring data breach lawsuits, while **legislation establishes private rights of action**

IRP Infrastructure Overview

Privacy+ Security Forum

- Appropriate **designation** of roles
- **Out-of-band** communication channels
- Understanding **contractual** notification requirements
- **Pre-selection** and **engagement** of incident response providers
- Detailed and practicable **escalation procedures**
- Coordination with **security partners**
- Tested **back-up and recovery procedures**
- Documentation of **critical containment and triage steps**
- Preservation of **evidence**
- Avoiding **configuration errors**

Appropriate Designation of Roles

Privacy+ Security Forum

- **Every** IRT should include:
  - Technical investigation lead
  - Executive liaison
  - Legal
  - Communications
    - Internal **and** external
  - Risk management
  - Executive decision-maker
  - Project manager(s)
- Every IRT member should have an **alternate**
- Consider **sub-teams** for large-scale incidents

Designate Alternate Comms Channels

Privacy+ Security Forum

- Corporate communications channels should **never** be assumed secure
- Designate **secure**, **out-of-band comms channels** for:
  - Virtual video conferencing
  - Email
  - Chat
  - Mass-messaging platform
- Establishing alternate channels in real-time **wastes valuable time**

Understand Notice Requirements

Privacy+ Security Forum

- Business partner **contracts**
- **Statutory/regulatory** frameworks
- **Insurance** policies
- Understand both **notice provisions** and available **coverages**
- Resources available to you through **insurance policies**

Pre-Select External IR Partners

Privacy+ Security Forum

- Vet your **cyber insurer's panel providers**
  - Breach/privacy counsel
  - Forensics/TA communications
  - Crisis communications
  - Notification
- Establish relationships **pro-actively**
- **Pre-negotiate** commercial terms

Establish Practical Escalation Procedures

Privacy+ Security Forum

- Understand the ways your organization may be **alerted** to a cyber incident
- Ensure **well-defined escalation procedures**, both **internally** and **externally**
- Role of **external security partners**

Coordination with Security Partners

Privacy+ Security Forum

- **Understand** the roles and responsibilities of your:
  - EDR Provider
  - SIEM/SOC
  - MSSP
- **Pro-actively** discuss with them **roles and expectations**

Test Back-up and Recovery Procedures

- Establish **back-up verification process**
- Test the **time** to restore from backups
- Consider **contingencies and dependencies** to restore
- **Offline** backups
- Taking **snapshots**

Critical Containment and Triage Steps

- Prepare a **network diagram**
- **Isolate** affected systems
  - **Do not** power down unless necessary
- **Disable** user accounts
  - **Do not** delete accounts or data
- **Preserve** ephemeral data
- **Reset**:
  - **Privileged account** passwords
  - **Service account** passwords
  - **Golden ticket**
- Develop a **plan** for resetting user credentials

Preservation of Evidence

Privacy+ Security Forum

- Understand **log retention periods**
  - Best practices for **retention**
- **Preserve** logs for:
  - **Firewall** (traffic/intrusion detection)
  - **Remote** access/**VPN**
  - **Critical** systems
  - **Security** tools
  - **EDR** reports
  - **MFA** logs
- Take **images** of impacted systems

Prevention - Avoiding Configuration Errors

Privacy+ Security Forum

- Patch management
- EDR/MDR
- Remote access/perimeter services
- Business Email Compromises
  - M365 licensing
  - OneDrive/SharePoint
- Multi-Factor Authentication
  - Legacy v. Modern
- Adversary-In-The-Middle Attacks
  - SMS/MITM attacks
  - New authenticators
- Applications in M365

Speakers

Privacy+ Security Forum

Elizabeth (Liz) R. Dill

Partner & Co-Chair, Advisory Compliance
Mullen Coughlin LLC

Matt Ahrens

VP, Forensic Services
Charles River Associates (CRA)