Robinson+Cole

Anatomy of a Data Breach

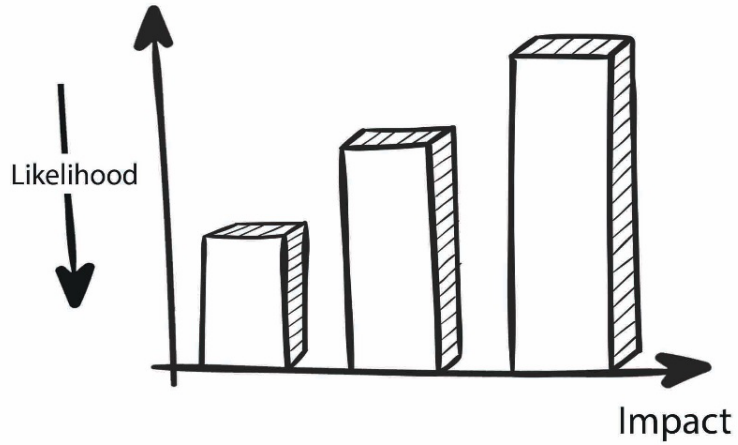
Nancy Cohen, Data Privacy Program Manager (Textron)
Paul Smith, President (Datasmith Network Solutions)
Kathryn Rattigan, Esq. (Robinson + Cole)

February 16, 2023

Introduction

Headline-grabbing breaches and shutdowns have put manufacturers of all sizes on notice that everyone is vulnerable and no one—no matter how small or large—escapes the interest of cyber attackers.

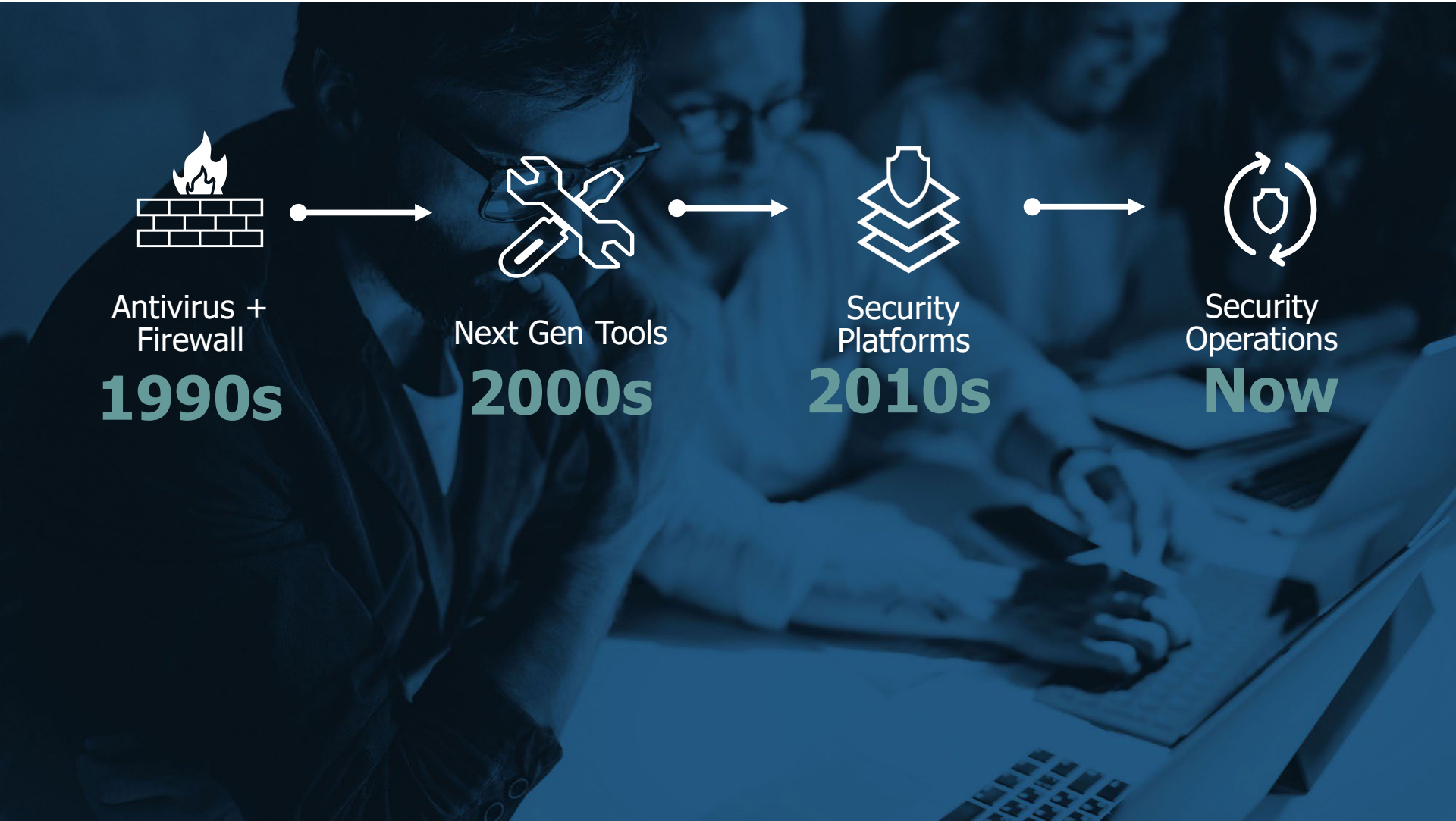
What you need to know about Security



The Criminal

YouTube video link:
https://youtu.be/AyTHVcds6_0

Finding the Right Approach



Too Many Alerts

CISO Benchmark Survey

Most teams face more than 10,000 alerts per day

They only investigate half (51%) of them

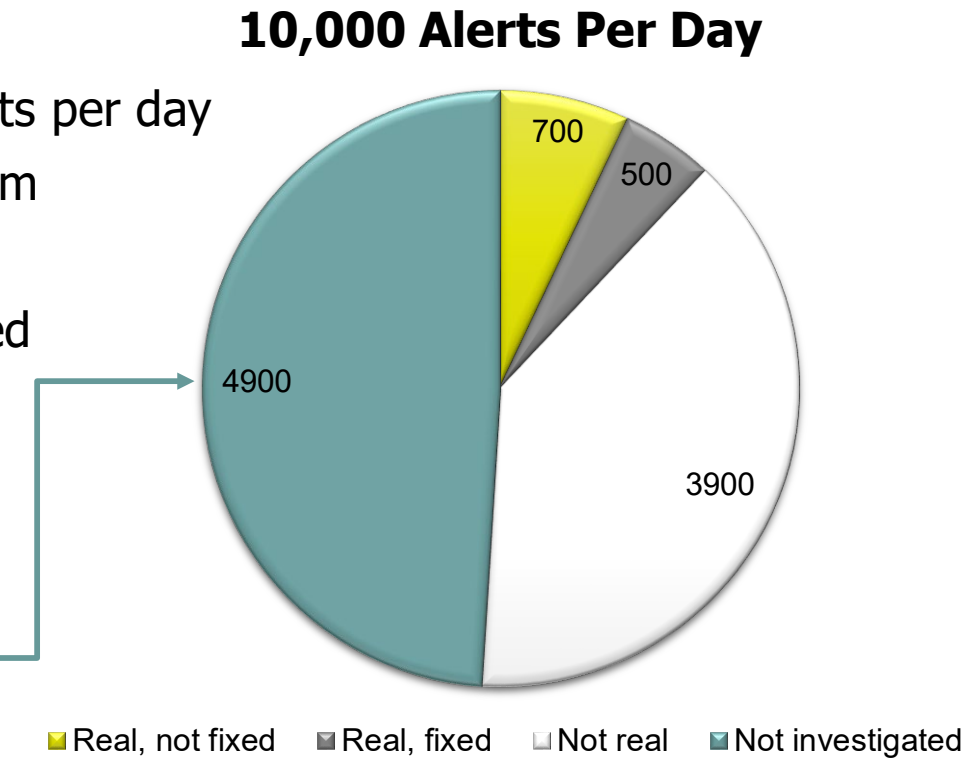
Of those, only 24% are real threats

Of those real threats, only 43% get fixed

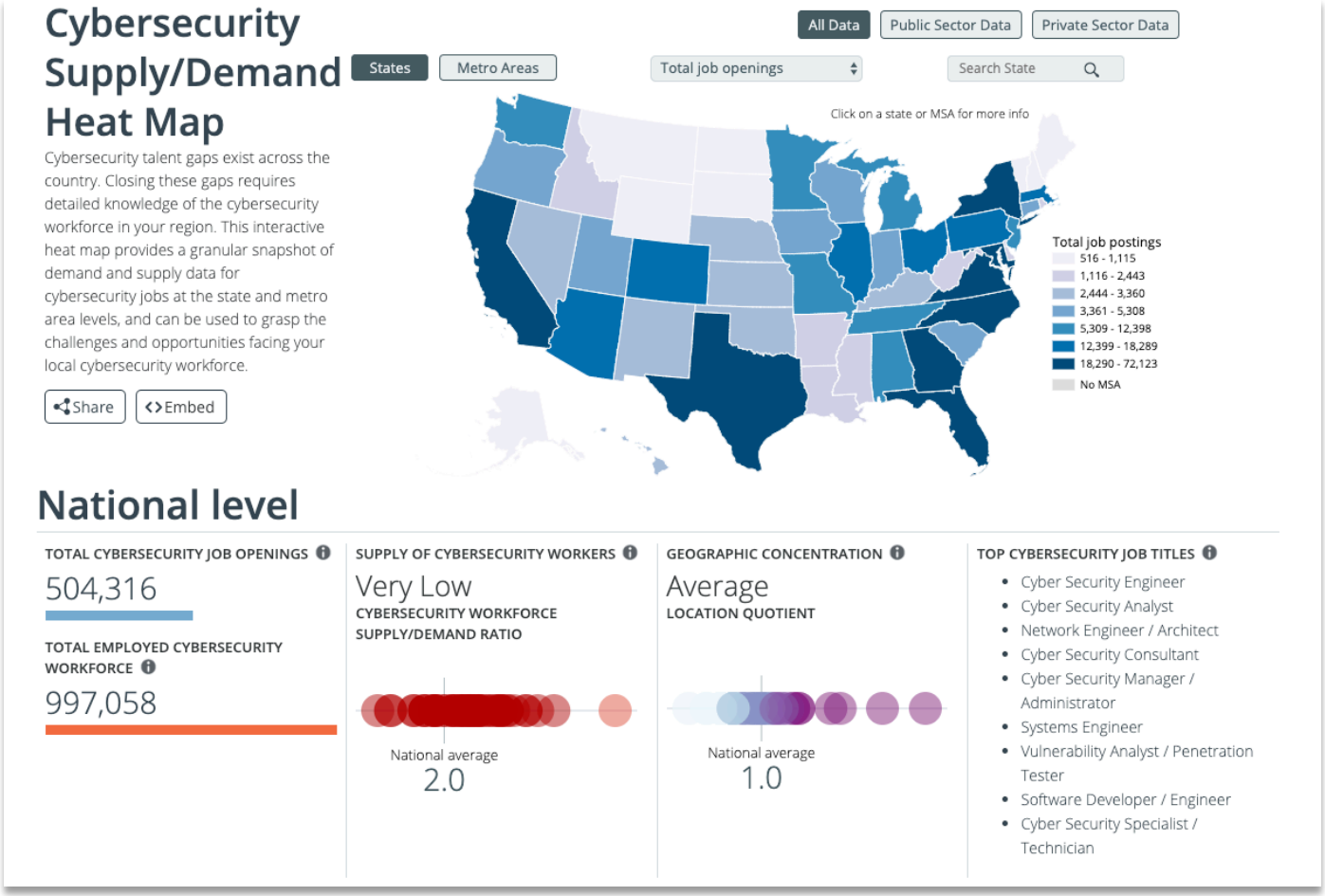
No wonder dwell time is so long!

How many of the uninvestigated alerts contained a real threat?

... we will never know because they didn't investigate

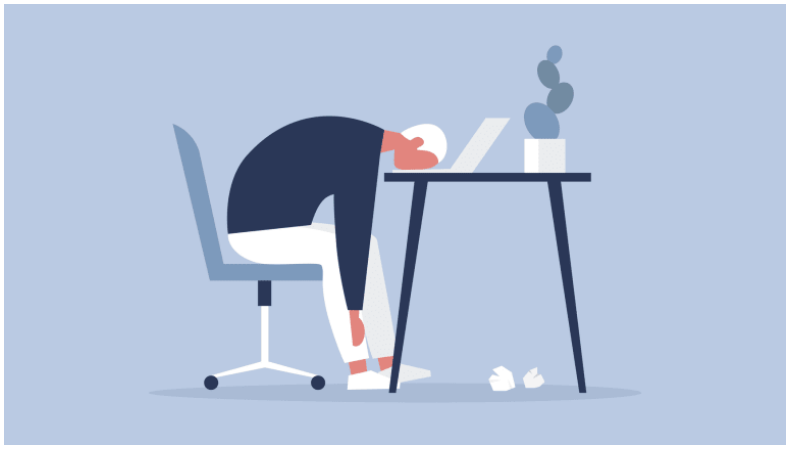


Not Enough People



- Organizations lack needed security experts
- Global skills shortage; 3.5M unfilled jobs by ‘22
- Hyper-competition makes retention difficult
- Skill atrophy leaves teams unprepared
- Feel “under water,” so too busy to strategize

Burnout



CISO Stress Report – 48% of CISOs said their work stress has impacted their mental health, and 35% said it has impacted their physical health.

- **Little time to decompress** – sheer volume of security alerts
- **Simmering frustrations** – understaffed, lacking budget, wayward employees
- **Exhausting schedules** – always being "on the job"

What is the problem?

Operational Model

Vulnerability Discovery – *Terms to Know*

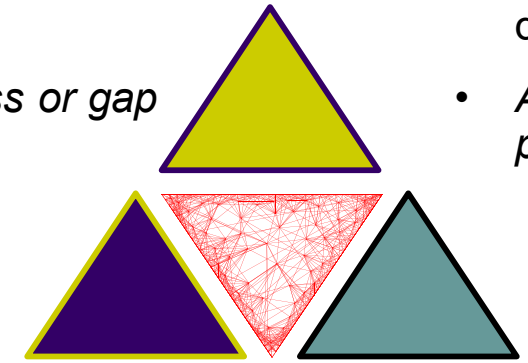
What are assets, vulnerabilities, threats and risks?

VULNERABILITY:

- Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.
- *A vulnerability is a weakness or gap in our protection efforts.*

THREAT:

- Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset
- *A threat is what we're trying to protect against*



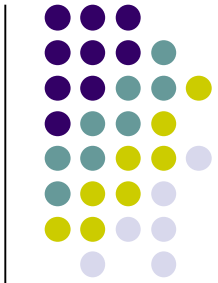
ASSET:

- People, property, and information
- *An asset is what we're trying to protect*

RISK:

- The potential for loss, damage or destruction of an asset because of a threat exploiting a vulnerability
- *Risk is the intersection of assets, threats, and vulnerabilities*

Let’s Recap



- Too many alerts
- Not enough people
- Continuation of breaches, with escalating consequences
- Too many products to consider
- Cloud is only making it harder
- 5 Step Operational Model
- Where are your Vulnerabilities

What are the top risks?

- Phishing/Spear-Phishing
- Zero-Day Vulnerabilities
- Ransomware Attacks
- Supply Chain Attacks
- Nation-State Attacks
- IP Theft –trade secrets –the “crown jewels”
- Equipment Sabotage
- Telecommuting Risks

Trends to watch for in 2023

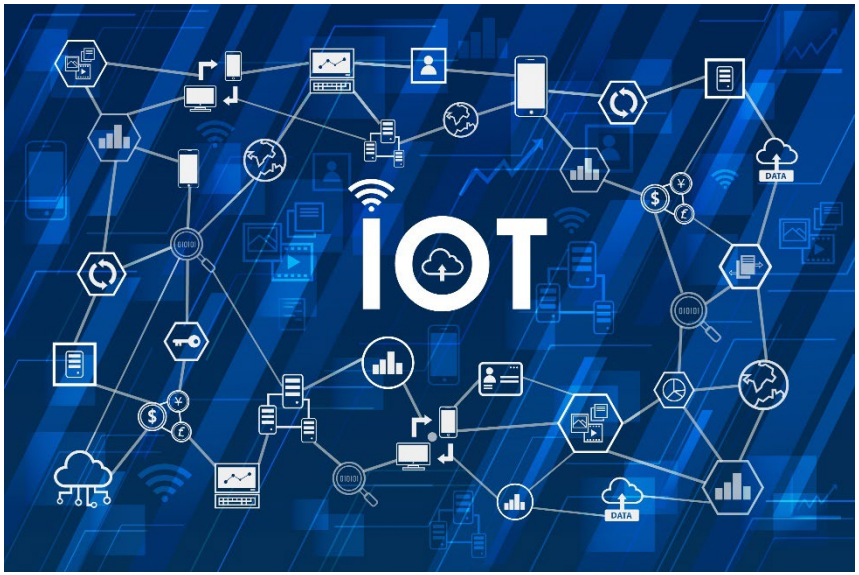
- **Hackers are targeting infrastructure**
  - Nation-state and terror organizations are increasingly targeting critical infrastructure to destabilize communities.
  - Cybersecurity and Infrastructure Security Agency (CISA) warns that manufacturing control systems are critical infrastructure.
  - Targeted disruptions in key manufacturing sectors could cause widespread shortages due to the interconnected global supply chain.

Trends to watch for in 2023 (cont'd)

- **Ransomware is franchising**
  - Ransomware groups are beginning to pivot to a ransomware-as-a-service model, leasing their software out to unsophisticated opportunists.
  - Even if the organization pays, the targeted data may still be lost due to the extortioners' unfamiliarity with the tools.
  - Ransomware groups have adopted the "double extortion" model, where they both encrypt the data on the company's servers and threaten to post the data on publicly accessible dark web forums.

IoT and Manufacturing Control Systems

- IoT products as attack vectors
  - Manufacturing plants are increasingly integrating Internet-of-Things (IoT) devices into their manufacturing control systems, increasing the organization's attack surface.



Wire Transfer Fraud

- The valid email account of the manager, employee or vendor is hacked and the hacker makes a request for either fraudulent wire transfers for what appeared to be valid payments to vendors or changes to payroll ACH transactions.

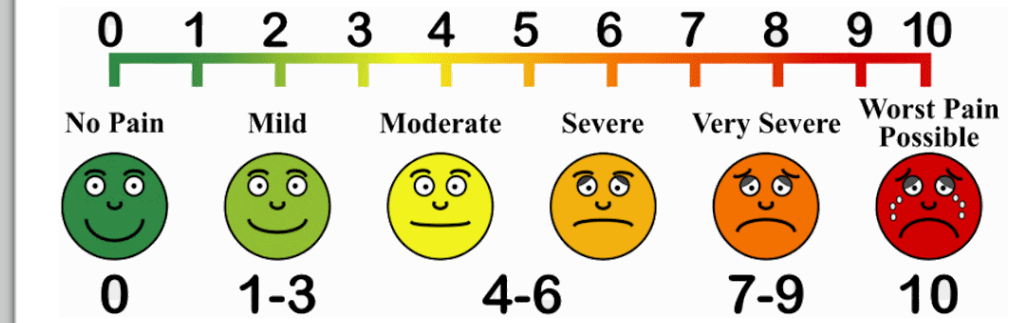
But what happens WHEN a security incident occurs?

CHALLENGES AND BEST PRACTICES

SECURITY INCIDENT CHALLENGE #1

Panic

- Confusion surrounding incident response procedures
- Worries about getting fired or in trouble
- Delayed response



TEXTRON

SECURITY INCIDENT CHALLENGE #2

Communication Failures

- Stakeholder powerplay
- Roles/responsibilities not mapped out

TEXTRON

SECURITY INCIDENT CHALLENGE #3

Budget

- Combating security incidents with limited tools
- Spending after an incident instead of prior
- Paying ransom to get back to business as usual

TEXTRON

SECURITY INCIDENT CHALLENGE #4

Data Overload

- Data cemeteries
- Personal data field confusion
- Retention guidelines not followed

TEXTRON

SECURITY INCIDENT CHALLENGE #5

Resources

- Accepting help from law enforcement, outside counsel, forensic firms

TEXTRON

BEST PRACTICES

- Don’t Panic
- Know your role and responsibilities regarding security incidents
- Accept help from outside sources (outside counsel, law enforcement, etc.) if available to you
- Follow record retention guidelines
- Ensure customer/employee personal data is collected, stored, transferred, shared and deleted in accordance with company policies and the legal requirements
- Speak up promptly if you become aware of any loss, misuse or unauthorized access of personal data – deadlines on reporting incidents
- Don’t leave personal data lying around on a desk or unattended on a computer screen
- Don’t send any files with Personal Data that are not encrypted or otherwise password protected
- Conduct education and awareness training on incident response plans

Remember!

Privacy is a forethought and not an afterthought!!

What can you do to be proactive?

Implementation of an Incident Response Plan

- The **Plan** is designed to provide a well-defined, organized approach for handling any potential security breaches, or threats to data, systems, and infrastructure.
- The **Plan** defines what constitutes a security incident, identifies the areas of responsibility, establishes a process for documenting the incident and includes assessment procedures.

Implementation of an Incident Response Plan (cont'd)

- **Determine who are the stakeholders:**
  - Organizational leadership
  - IT & Information Security leadership
  - Audit
  - Finance
  - Human Resources
  - Communications
  - Legal counsel

- **Determine what decisions need to be made:**
  - Obtain or clarify cyber liability insurance information and requirements
  - Determine vendors needed such as forensics, outside legal counsel, mitigation and communications services

Implementation of an Incident Response Plan (cont'd)

Objectives:

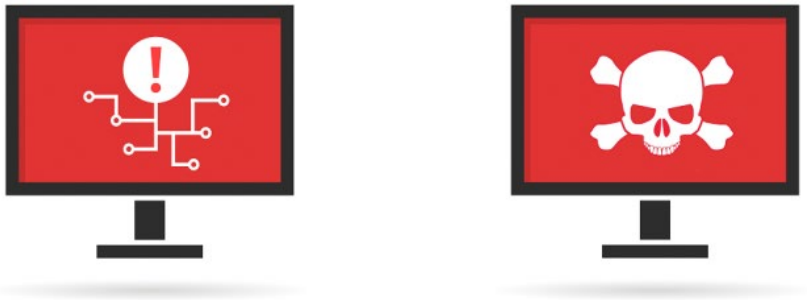
- Conduct investigation into incident
- Coordinate response to incident
- Establish communication protocols
- Provide notice to appropriate regulatory authorities
- Coordinate with third-party service providers
- Act as liaison to law enforcement or information sharing agencies, including state and federal
- Determine notice requirements – to any affected individuals

Implementation of an Incident Response Plan (cont'd)

- **Compile the following information NOW:**
  - Obtain and select insurance approved vendors (as appropriate) and maintain updated contact information for:
    - Forensic vendors
    - Credit monitoring/call center/identity theft mitigation services vendors
    - Outside legal counsel
    - Cyber insurance broker and insurance company contact information to report a breach/security incident
    - Law enforcement officials, including state and federal officials
    - Applicable regulatory body
    - Information sharing entities
  - Distribute the Plan and review it at least once annually
  - Conduct tabletop exercises

How to Avoid Phishing Schemes and Ransomware Attacks

- Be aware of any urgent or confidential requests.
- Think before replying – Never "reply" or click on unknown links in emails containing a suspicious request or open suspicious attachments in emails that you weren't expecting to receive or that seem odd.
- Authenticate the sender of the message by contacting him/her by an alternative method – Contact a different person before sending sensitive information or authorizing transactions.
- Update and patch systems and make sure security solutions are up to date.
- Be mindful of what you share on social media and regularly update your privacy settings.
- Install and enable remote wiping and/or remote disabling of computer devices.



Practice Proactive Protection and Prevention

- Create and implement a Written Information Protection Plan (WISP)
  - Include regular audits of all security policies
- Require third-party partners to safeguard sensitive data = vendor management
- Secure data breach insurance
- Foster a security-conscious work environment

Questions? Contact Us

Would you like some help?
Let Paul assist in guiding you with a 1-hour consultation at no charge.
psmith@datasmithnetworks.com

SCAN ME

Kathryn M. Rattigan
krattigan@rc.com
Robinson + Cole
One Financial Plaza
14th Floor
Providence, RI 02903
401-709-3357

Subscribe to Robinson + Cole's privacy and security blog at www.dataprivacyandsecurityinsider.com

Data Privacy Program Manager & Corporate FSO
Textron Inc.
40 Westminster St.
Providence, RI 02903
401-457-3651