Robinson+Cole

Cyberattacks, ransomware and the current state of cyber risks

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS (NEHIA)
HEALTHCARE FINANCIAL MANAGEMENT ASSOCIATION (HFMA)
ANNUAL COMPLIANCE AND AUDIT CONFERENCE

Linn Foster Freedman, Esq.

December 1-3, 2021

Overview

- Healthcare Industry as a Target
- High-Risk Data
- Current Trends in Cyber Threats
  - Ransomware Attacks
  - Recent Attacks in the Healthcare Industry
- How a Healthcare Organization can Protect its Systems and Data
  - Incident Response: Planning, Mitigating and Post-Incident Review
- Tips for Protecting Against these Threats
- Conclusion

Introduction

Ever-increasing threats to privacy and cybersecurity present serious challenges for the healthcare industry.

Health Care and Technology

- The effects of power outages on hospitals caused by the collapse of public power grids or the destruction of generators due to modifying code in controllers would have devastating consequences for patient care.
- There are also more subtle threats such as the theft or loss of patient information, disruption of care due to software outages, or loss of confidence in health care providers due to perceptions of inadequate security.

What data is the most high-risk?

Identifying and Protecting High-Risk Data

- Social Security number
- Driver's license number or state-issue identification card number
- Passport number
- TIN/EIN
- Alien registration number or tribal identification number
- Financial account number, credit card number, or debit card number with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account, or deposit or savings account number

Identifying and Protecting High-Risk Data (cont'd)

- Medical or health insurance information (including protected health information under HIPAA/Part 2 substance use disorder treatment information)
- Username or email address in combination with security code, access code or password or security question and answer that would permit access to an online account
- Biometrics
- Research/Proprietary Formulas, Technology Plans/Schematics

Current Trends in Cyber Threats

The average time to identify and contain a breach

is 280 days. (*2020 Ponemon Report*)

Average Cost of a Data Breach in 2020

- $3.86 million
  - Having a remote workforce was found to increase the average total cost of a data breach by nearly $137,000, for an adjusted average total cost of $4 million.

HOWEVER

$7.13 million was the average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study.

(***2020 Ponemon Report***)

Current trends - What is the threat landscape?

- **What are the threats to healthcare organizations' operations, infrastructure and/or data?**
  - Unintended disclosures by employees; Employee Error
  - Hacking/Malware/Ransomware
  - Insider Wrong-Doing
  - Zero Day Vulnerabilities
  - Physical Loss
  - Portable Device/Removable Media

Current trends – threat landscape (cont'd)

- Technology Intrusions
- Phishing/Spear-Phishing Schemes
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Vendors/Subcontractors –Poor Security Protocols/Standards

Risks to Data

- **Phishing**
  - A malicious "spam-like" message sent in large batches to broad audience
    - Includes **Smishing** (i.e. exploitation via text message)
- **Spear-Phishing**
  - A form of phishing – messages appear to come from a familiar or trusted sender and target recipients
- **Ransomware**
  - A type of malicious software designed to block access to a computer system until a sum of money is paid
- **Malware**
  - Software that is intended to damage or disable computers and computer systems

Phishing

Phishing is an attempt to steal personal information. Most times it involves an e-mail, although other forms of communication can be used, which claims to be a legitimate business or person in an attempt to scam you into surrendering personal information, financial information or downloading malicious software.

Be suspicious of any email that:

You were not expecting to receive

- Requests personal information (account numbers, SSN, username, passwords, birth date, etc.) or financial information
- Requires you to urgently take action (e.g., verify your account or log-in to prevent your account from being closed; make payment for an outstanding invoice)
- Does not look like a legitimate business Website (e.g. logos look funny, spelling errors)
- Has a different URL than the one you are familiar
- Contains a document that shuts down and re-launches after you open it

Spear-Phishing

- **Spear phishing** is an email that appears to be from an individual, business, or department that you know. But it isn't. It's from the same criminal hackers who want credit card and bank account numbers, passwords, and the financial information on your computer.
- Form of social engineering
- **The criminal thrives on familiarity.**
  - **e.g. an email from someone who is pretending to be your CEO or IT personnel**

Vishing and Smishing

- Exploits via SMS, telephone calls or text, messages
- Vishing
  - Often the caller will pretend to be calling from the government, tax department, police, or a bank, requesting personal information
- Smishing
  - Text messages can contain links to such things as webpages, email addresses phone numbers that when clicked may automatically open a browser window or message or dial a number
- Cyber criminals want this integration of email, voice, text message, and web browser functionality to increase the likelihood that we will fall victim to engineered malicious activity

Malware

- Malware is any software intentionally designed to cause damage to a computer, server, or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of:
  - Computer viruses
  - Worms
  - Adware
  - Spyware
  - **Ransomware**
  - Bots
  - Rootkits
  - Trojan Horses

Ransomware

- Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid (usually in bitcoin).
- Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/patients.

Recent Ransomware Attacks

- The line between ransomware attacks and data breaches continued to blur in 2020 and now in 2021, with a number of prolific ransomware operators – including **Maze, Sodinokibi (Revil), DoppelPaymer, Nemty, Nefilim, CLOP and Sekhmet** – creating their own websites where they publish the stolen data of non-paying victims.

Ransomware Threats (cont'd)

- In 2020, **Maze**
  - To have leverage over organizations, these hackers stole data from the infiltrated system while it deployed the ransomware. They then threatened to publish the data if the victim decides not to pay.
- In 2021
  - **Phobos**
    - Distributed via hacked Remote Desktop Protocol (RDP) connection
  - **CloP**
    - Phishing campaign

Ransomware Statistics

- Coveware issued its Q1 2021 Ransomware Report on April 26, 2021
  - "[D]ata exfiltration extortion continues to be prevalent and we have reached an inflection point where the vast majority of ransomware attacks now include the theft of corporate data."

Ransomware Statistics (cont'd)

- The average ransom payment increased by 43%
  - $154,108 in Q4 2020 to $220,000 in Q1 2021
- The median ransom payment increased by 58%
  - $49,450 in Q4 2020 to $78,398 in Q1 2021
- According to Coveware, the activity by CloP in Q1 2021 was "extremely active"

Ransomware Statistics (cont'd)

- 77% of all threats included the threat to leak exfiltrated data, which was an increase of 10% from Q4 2020
- Sodinokibi continued to dominate the market share as a ransom type at 14.2%, followed by Conti V2, Lockbit, CloP, Egregor, Avaddon, Ryuk, Darkside, Suncrypt, Netwalker, and Phobos
  - Of these, Egregor has sunset its operations, and Netwalker was dismantled by law enforcement.
  - Darkside behind Colonial Pipeline attack.
- The top vectors for attacks included remote desktop protocol compromise, "phishing emails that install credential stealing malware," software vulnerability, and vulnerabilities in VPN appliances

Coveware Q3 Report

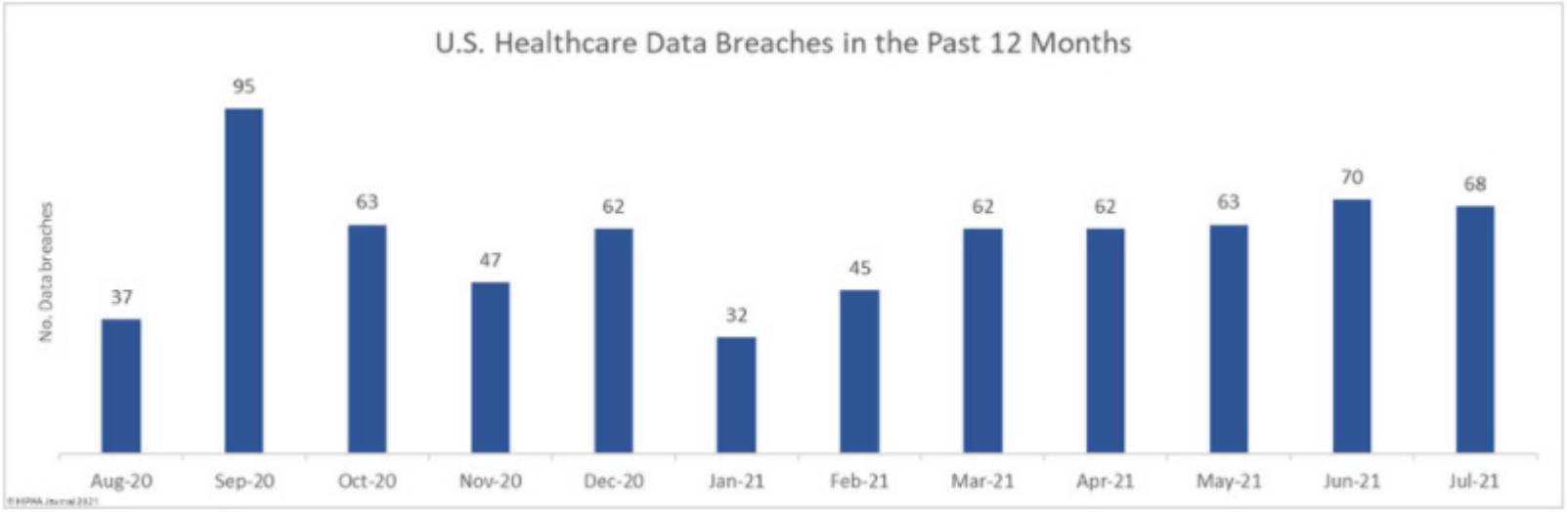
- Ransomware and data exfiltration tactics “remain intertwined”
- 80% of ransomware attacks involve theft of data and file encryption
- Credential access continues to be the #1 attack vector
- Attackers are now targeting mid-sized companies
- Health Care entities third most hit industry

What are the Effects of these Threats?

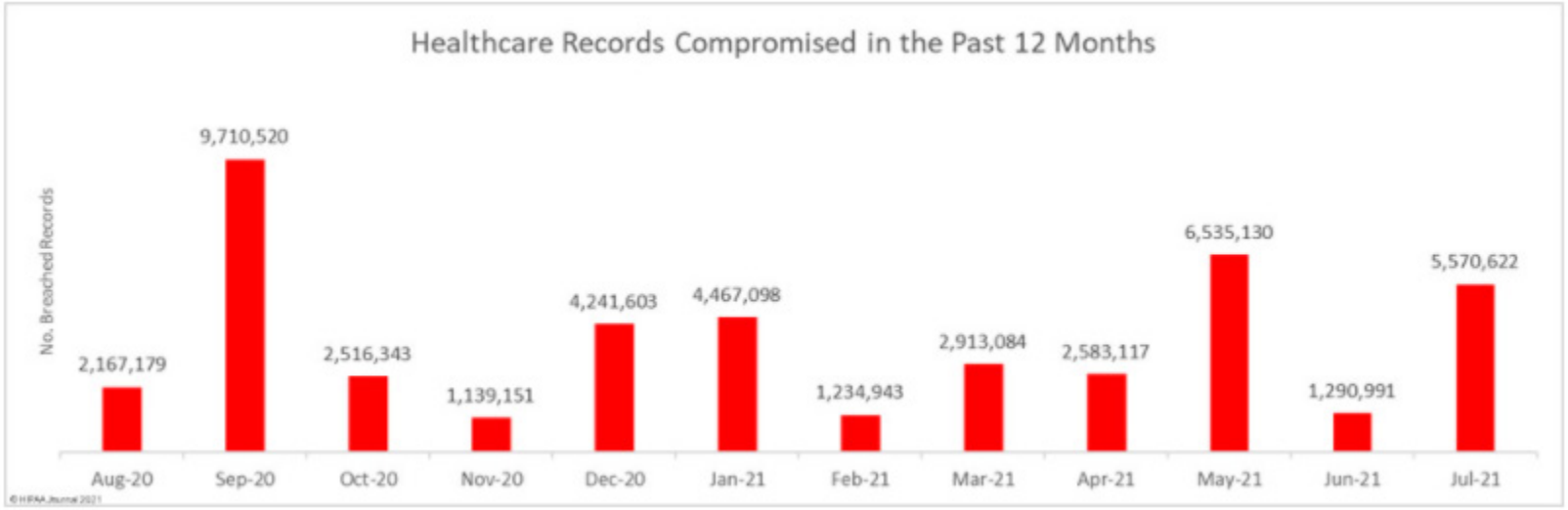
- Traditional cyber threats to businesses present a range of damages that include reputational damage, financial gain and fraud, commercial advantage.
- Any and all of these activities could disrupt the providing of health resources through an inability to produce needed medical equipment or drugs through manufacturing stoppages, loss of PHI and subsequent decreases in public trust of health apparatuses, or failures of vendors to provide key hospital services that might range from software to temporary staffing.
- Potential to remotely access and damage physical systems is another threat.

The above-noted threats, if they occurred in businesses critical to public health infrastructure, could shut down or slow supply chains, impair patient care, and impede emergency response, potentially leading to significant loss of life.

Attacks on the Health Care Sector



Attacks on the Health Care Sector (cont'd)



Recent Attacks and the Cause

Forefront Dermatology, S.C.	Healthcare Provider	2,413,553	Hacking/IT Incident	Unspecified hacking incident
Professional Business Systems, Inc., d/b/a Practicefirst Medical Management Solutions/PBS Medcode Corp	Business Associate	1,210,688	Hacking/IT Incident	Ransomware attack
UF Health Central Florida	Healthcare Provider	700,981	Hacking/IT Incident	Ransomware attack
Orlando Family Physicians, LLC	Healthcare Provider	447,426	Hacking/IT Incident	Phishing attack

Recent Attacks and the Cause (cont'd)

Coastal Family Health Center, Inc	Healthcare Provider	62,342	Hacking/IT Incident	Ransomware attack
Florida Heart Associates	Healthcare Provider	45,148	Hacking/IT Incident	Ransomware attack
A2Z Diagnostics, LLC	Healthcare Provider	35,587	Hacking/IT Incident	Phishing attack
University of Maryland, Baltimore	Business Associate	30,468	Hacking/IT Incident	Unspecified hacking incident
Florida Blue	Health Plan	30,063	Hacking/IT Incident	Brute force attack (Member portal)
Intermountain Healthcare	Healthcare Provider	28,628	Hacking/IT Incident	Ransomware attack (Elekta)

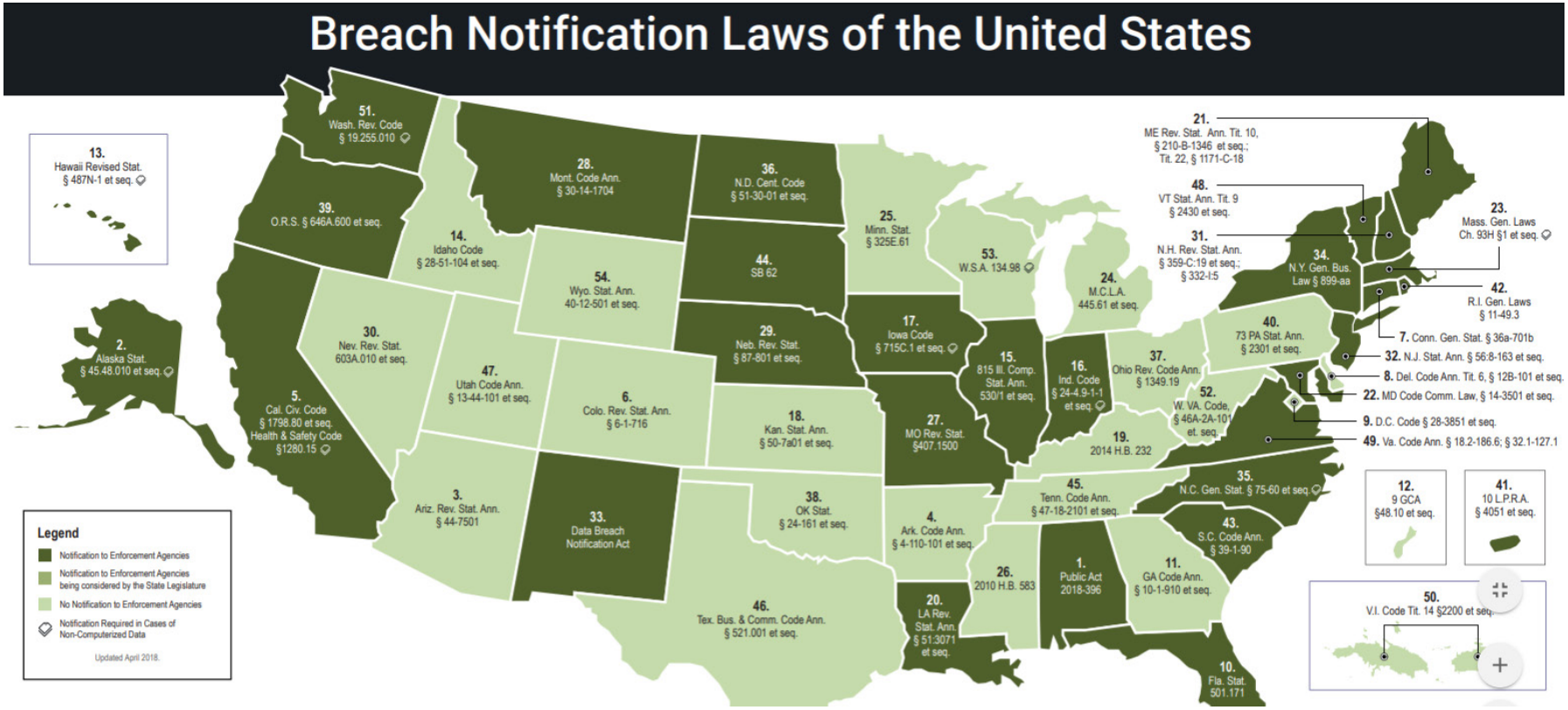
Recent Attacks and the Cause (cont'd)

HealthReach Community Health Centers	Healthcare Provider	122,340	Improper Disposal	Improper disposal of electronic medical records
Guidehouse	Business Associate	84,220	Hacking/IT Incident	Ransomware attack (Accellion FTA)
Advocate Aurora Health	Healthcare Provider	68,707	Hacking/IT Incident	Ransomware attack (Elekta)
McLaren Health Care Corporation	Healthcare Provider	64,600	Hacking/IT Incident	Ransomware attack (Elekta)

What are the Legal Obligations in the event of an Attack?

- HIPAA/HITECH
- State Law (not all states have an exception for HIPAA or the data may not be considered PHI
  - e.g. Blackbaud breach –donor information

50 State Data Breach Notification Laws

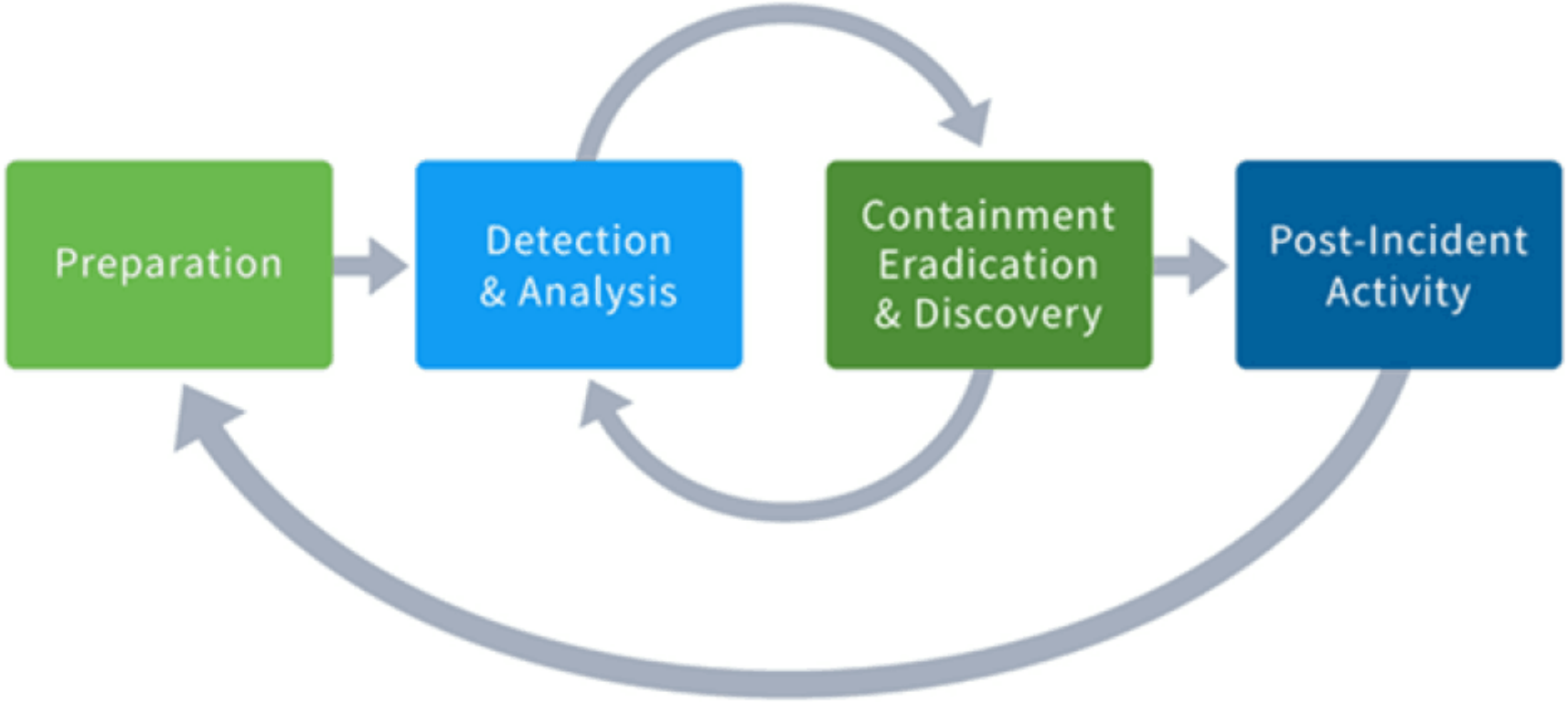


OCR Enforcement Actions in 2021

- 20 settlements for Right of Access Initiative
- Settlement for $5.1M for data breach affecting 9.3 million people
  - Hacker gained access to system—failure of access controls
- Settlements for Security Rule Violations
  - Commented that failure to implement basic Security Rule requirements “makes HIPAA regulated entities attractive targets for malicious activity”

Incident Response Plan: What is it and why do you need one?

NIST: Recommended phases for responding to a cybersecurity incident



Preparation: Developing the Incident Response Plan ("the Plan")

- The **Plan** is designed to provide a well-defined, organized approach for handling any potential security breaches, or threats to your 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.

Preparation: Who needs to be part of the Plan development team?

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

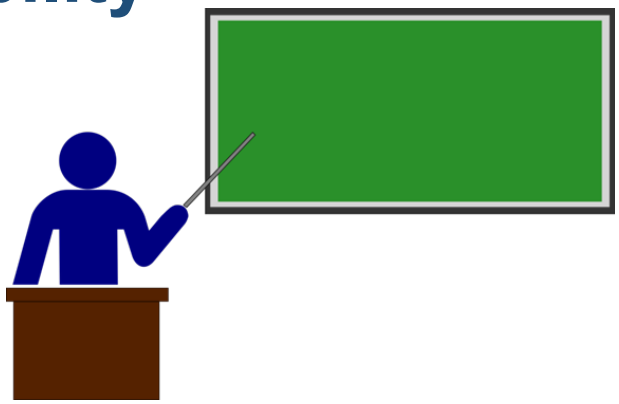
- **Determine what decisions need to be made:**
  - Obtain or clarify cyber liability insurance information and requirements
  - Determine vendors needed such as forensics, outside legal counsel, mitigation and communications services

Preparation: Goals of the Plan

- Establish the **Incident Response Team** (the "Team")
- Establish **definitions** –security incident, data breach
- **Assess** the incident and threat level
- **Define** the actions to be taken when an incident occurs
- **Respond** to the incident
- **Restore** - present an orderly course of action for restoring functionality
- **Document** – collect and document the incident
- **Communicate** – specify how information should be communicated, who should communicate and how
- **Mitigate** – implement processes to mitigate the effects of the incident

Maintenance & Going Forward

- Determine who has responsibility for maintaining the Plan
- Make sure the Plan is distributed as appropriate, within the organization

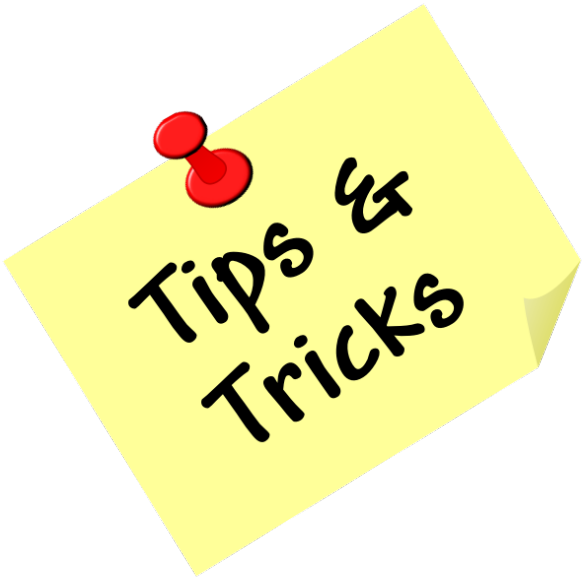


- Review Plan at least annually
- Conduct tabletop exercises at least annually
- Conduct regular staff, user and employee education and training in privacy and security

Summary of Actions to take Now

- Cybersecurity risk assessment – determine security gaps in systems and networks
- Implement prevention strategies – strong passwords multi-factor authentication, encryption for laptops, thumb drives, mobile device policies, including BYOD,
- Update software and implement regular patches
- Educate and train employees
- Vendor management
- Back up data
- Incident Response Plan
- Update IT/computer/cybersecurity policies and procedures
- Obtain/update cyber liability insurance

What can YOU do to avoid these schemes and attacks?



Tips to Avoid these Schemes and Attacks

- Read e-mails with an eagle eye
  - **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters. Hover over the email address to check this out.
  - **Generic greetings and signature**. Both a generic greeting-such as "Dear Valued Customer" or "Sir/Ma'am" – and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
  - **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

Tips to Avoid these Schemes and Attacks (cont'd)

(cont'd)

- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments**. An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

- Keep informed about phishing techniques
- Think before you click!
- Keep your browser up-to-date
- Be wary of pop-ups

Tips to Avoid these Schemes and Attacks (cont'd)

- On your mobile devices (cont'd)…
  - PRIVACY SETTINGS
    - Location, microphone

Increased Cyber Threats with Remote Working

- The Healthcare Sector is an attractive target –lots of sensitive, protected data.
- The risk of cyber breaches has multiplied due to working remotely.
- The pandemic created opportunities for hackers and scammers.
- There are still COVID-19/vaccination scams and malware sites being created daily.
- All work should be done on secure servers, using multifactor authentication and VPN to gain access to systems and information.

Tips for Remote Workers

Be wary of:

- Urgent email requests for personal information and/or confidential data;
- Technical support calling YOU claiming that your computer is infected;
- Vishing;
- Warning email that a package could not be delivered with a link to click to provide details;
- Unsolicited emails with a link to COVID-19 statistics in your area or other COVID related topics;

Tips for Remote Workers (cont'd)

Be wary of (cont'd)

- Unsolicited emails with a link to get a copy of your CDC vaccination card;
- A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.
- Be extra vigilant about phishing emails.

BETTER SAFE THAN SORRY!

Conclusion


health
insurance
care
system
people
healthcare
medical
companies
need
coverage
Get
One
pay
many
doctors
make
money
much
Government
costs
cost
Medicare
time
patients
just
like
years
plan
know
work
must
see
also
afford
even
ago
good
doctor
profit
take
without
services
benefits
private
way
New
better
problem
providers
change
life
provide
drug
country
treatment
children
needs
part
paid
well
patient
hospital
want
current
quality
single
expensive
access
healthy
cover
find
company
Americans
American
day
family
affordable
problems
hours
another
dollars
pharmaceutical
countries
program
based
enough
really
never
done
going
NOW
EVERYONE
less
illness
America
use
drugs
sick
year
education
National
Bill
medicine
back
industry
able
still
job
hope
something
food
making
believe
long
give
hospitals
may
paying
go
help
high
right
every
covered
available
conditions
state
first
business
World
payer
physicians
person
since
think
best
getting
keep
Obama
disease
etc
service
universal
public
big
working
free
premiums
made
things

Linn Foster Freedman
lfreedman@rc.com

Robinson + Cole
One Financial Plaza
Suite 1430
Providence, RI 02903
401-709-3353

Thank you

QUESTIONS?

www.dataprivacyandsecurityinsider.com