FORVIS

The State of Cybersecurity

Cindy Boyle

Meet the Presenter

Cindy Boyle, CPA, CIA, CITP, CISA
Partner
National Practice Leader – IT Risk and Compliance
FORVIS
Cindy.Boyle@forvis.com

FORVIS

Agenda

- Current Breach Data
- Risk Assessment
- Assessing Your Security
- Risk Mitigation
- Cyber Insurance
- Homework
- Q&A

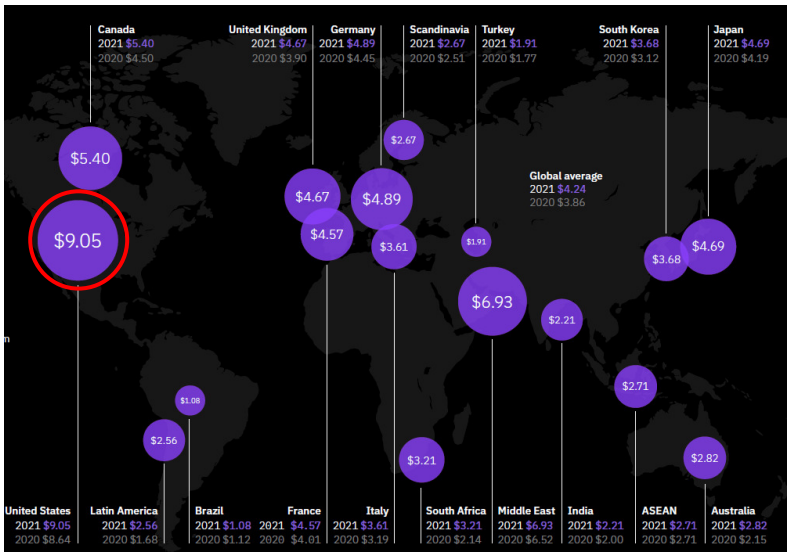
FORV/S

Current Breach Data

FORV/S

Breach Costs are up:

The United States leads total the cost of a data breach for the eleventh year in a row



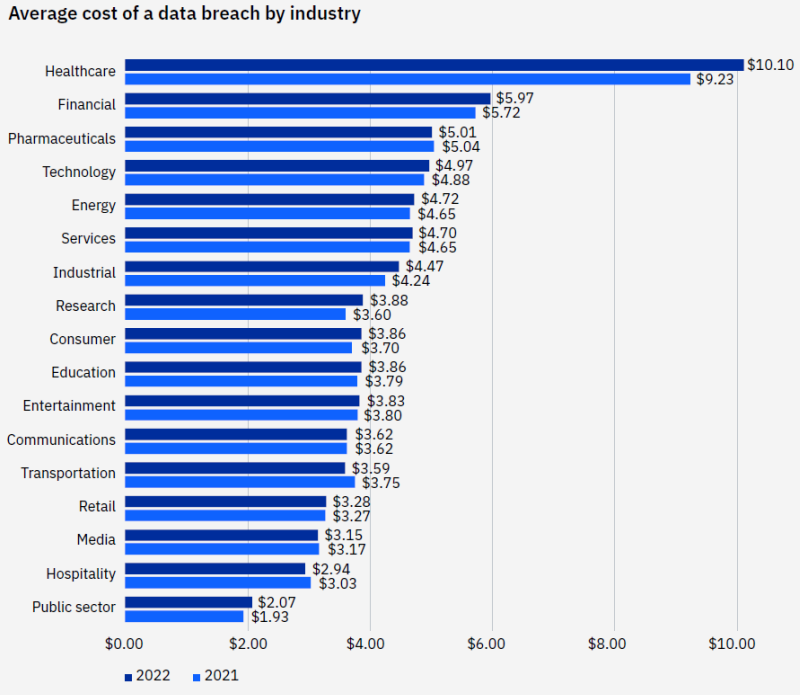
2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

5

Breakdown by Industry

Source: 2022 Cost of a Data Breach Report

FORVIS



Trending Issues

2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

FORV/S

Business Email Compromise (BEC)

FBI Internet Crime Report 2021

The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds or other malicious activities

Complaints:

19,954 - *Reported*

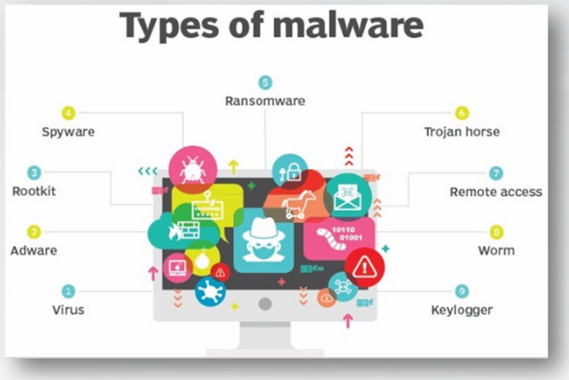
Losses:

Exceeding $2.4 billion

FORV/S

Most Common Cybersecurity Threats

- Social engineering attacks – phishing
- Malware/destructive malware
  - *Ransomware*
  - Remote access
  - Keyloggers
- Business email compromise
- Corporate account takeovers
- Supply chain!



Root causes of cyberattacks: Inadequate training, ineffective patch management, weak privileged access controls, & unmonitored detection systems

FORV/S

Ransomware Attack

Your personal files are encrypted

You have 5 days to submit the payment!!!

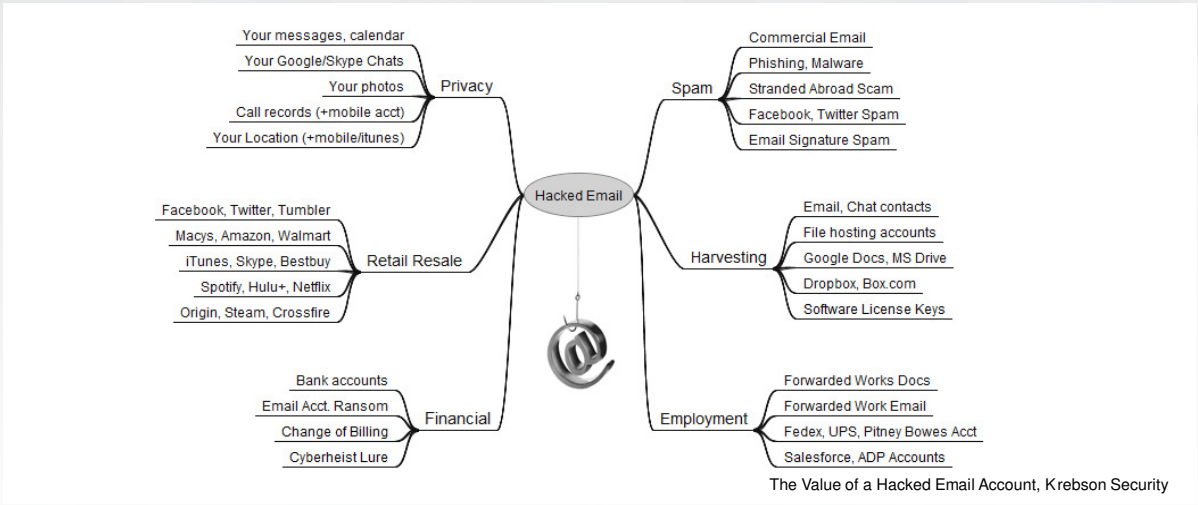
To retrieve the private key, you need to pay

Your files will be lost

FORV/S

10

The Ultimate Gateway – Email



The Value of a Hacked Email Account, Krebson Security

FORV/S

Athena

Dedicated Password Cracker

- We utilize Hashcat, power of the Nvidia video cards
- We have cracked complex passwords up to 16 characters
- Dictionary words easiest to crack
- Over 100 million passwords per second

FORV/S

Avoid These Common Password Pitfalls

Current month or season	A holiday	City or street where you are located
Child's name with a number (especially a birth year)	Name of a popular song/nursery rhyme/religious passage	"Password" or "I hate passwords"
Vulgarity or racial slurs	Name of Windows service	Name of common network protocols

CRACKED PASSWORDS
$central1
$$Zack$$
tommyh14!
pay$1596
Twins123%
qwert123Q!
gnik.Tk75
tyui-789
zxcv-5987

FORVIS

Single Biggest Risk? Users

Importance of Awareness Training

Users – Your own employees – An estimated 65% of breaches are caused by organizational users

C-level executives are 12 times more likely to be the target of social engineering attacks

Are ALL employees/contractors required to complete information security training?

FORVIS

Risk Assessment

FORV/S

The foundation of an information security program, is an information security risk assessment

Risk Assessments
The Value of Your Data to You

$4.62m

Average total cost of a Ransomware breach

- Daily business operations rely on data that may not be deemed critical
- Part of the evaluation risk is maintaining data classification assessments
- You **ARE** a target
- NOTE: The University of California San Francisco Health Paid $1.14M

FORV/S

17

Assessing Security/Risk in Our Daily Life

- **Dropping, breaking cracking the glass**
  - A protective case

- **Unauthorized access**
  - Pin, password, facial recognition

- **Saving contacts, photos, data**
  - Backup, iCloud

FORV/S

18

Personal Risk Assessment Test

FORV/S

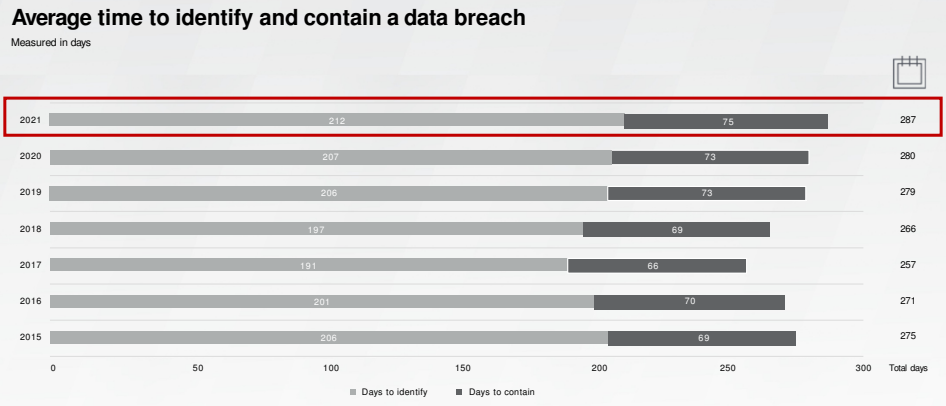
Remove your mobile device

Unlock it

Pass it to the person sitting next to you

Retrieve it at the end of this presentation

Reminder – Average time to detect a breach in the U.S.



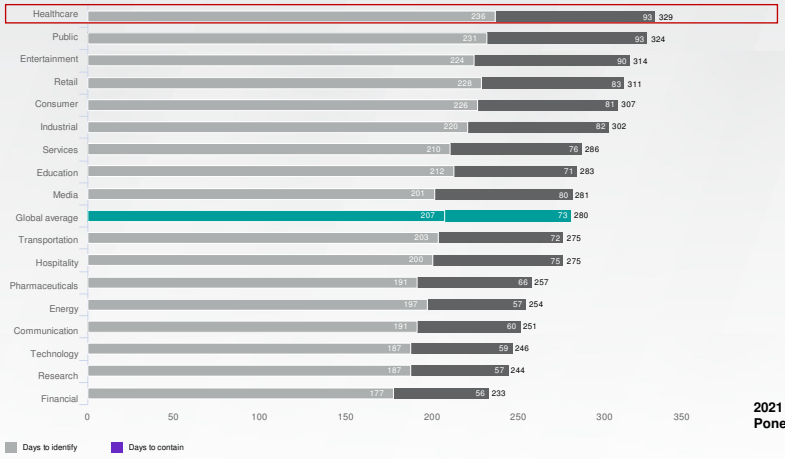
FORV/S

Average Time to Identify a Breach In Healthcare

Figure 36

Average time to identify and contain a data breach by industry

Measured in days



2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

FORV/S

Assessing Your Security

FORV/S

HIPAA Compliance

- The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information (ePHI) – not prescriptive
  - 347 breaches report to OCR in first half of 2022

HIPPA Compliance

FORV/S

Health Information Trust, Common Security Framework (HITRUST) CSF

HITRUST CSF is a certifiable framework with a list of prescriptive controls and requirements that can be used to demonstrate HIPAA compliance

HITRUST®

FORV/S

The HICP publication provides:

- Practical, cost-effective practices that will help strengthen your organization against cyber criminals
- Methods to integrate cybersecurity into your team's day-to-day operations, and;
- Outline an effective strategy to reduce your enterprise's cybersecurity risk

FORV/S

Health Industry Cybersecurity Practices (HICP)

HHS 405(d)
Aligning Health Care Industry Security Approaches

Source: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

25

Source:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

What is HICP?

- HICP was created by some of the most influential industry organizations in healthcare who came together and formed the 405(d) Task Group in May 2017, to plan and develop this publication
- They focused on
  - The five most prevalent cybersecurity threats and;
  - The ten cybersecurity practices needed to significantly enhance security for a broad range of organizations within the healthcare sector
- Recommendations in the HICP are based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework—the gold standard of cost-effective cybersecurity best practices

FORV/S

26

What are the Five Threats?

1. E-Mail Phishing Attacks;
2. Ransomware Attacks;
3. Loss or Theft of Equipment or Data;
4. Insider, Accidental, or Intentional Data Loss; and
5. Attacks Against Connected Medical Devices

Source: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

FORVIS

27

What are the 10 Best Practices?

1. E-Mail Protection Systems;
2. Endpoint Protection Systems;
3. Access Management;
4. Data Protection and Loss Prevention;
5. Asset Management;
6. Network Management;
7. Vulnerability Management;
8. Incident Response;
9. Medical Device Security; and
10. Cybersecurity Policies

Source: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

FORVIS

28

Where Do We Fit?

Using Table 1 on page 11 of the Main Document, organizations can determine their prescribed Technical Volume to use

Small, Medium, or Large

Best Fit		Small	Medium	Large
Common Attributes	**Health information exchange partners**	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	**Size (provider)**	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Table 7. Cybersecurity Practices and Sub-Practices for Small Organizations

29

Risks Mitigation

FORVIS

Key Considerations: Focus on Governance Controls

- Maintain a strong **information security program**
- Maintain a strong **incident response program**
- Ensure **business continuity/DR** & **vendor management** policies & procedures address cybersecurity
- Consider how **cybersecurity insurance** should fit into your risk management program
- Ensure **cybersecurity awareness training** is performed regularly (educate & motivate)
- Join **an information sharing & analysis center (ISAC)** or other information sharing forums – filter reports based on each employees' role
- Perform **frequent cyber risk assessments**, penetration tests, vulnerability assessments, & IT control audits

FORV/S

Key Considerations: Focus on Technical Controls

- Use **multifactor** or **two-factor** for O365, VPN, remote sessions, & privileged access
- Track, report, independently test, & update security **patches** based on a risk priority schedule (Microsoft & non-Microsoft patches)
- Maintain accurate **asset inventories** for hardware & software, including **data classification**
- Enforce **application whitelisting** controls & **remove** unauthorized applications
- **Remove local administrator** rights to reduce malicious software installs
- **Tune existing security tools** – web content, email filtering, end point, etc.
- Deploy **cloud-based security** software & end-point protection (SentinelOne, Crowdstrike, Windows Defender, etc.)

FORV/S

Key Considerations: Technical Controls

- Implement strong cloud-based **data loss prevention** controls
- Use **security information & event management (SIEM)** tools with **"defense in depth"** approach
- **Change** your passwords more frequently during this time
- Ensure **data encryption** is enforced to protect confidential data
- **Segment** internal networks to isolate critical systems
- Be aware of **insider threat** – layoffs, disgruntled, etc. Think zero trust!
- **Air gap** your backups to keep them out of reach of an attack
- Make your air-gapped backups **immutable**!

FORV/S

"We Have Cybersecurity Insurance"

So, we're covered right?

FORV/S

Cybersecurity Insurance

- Policy applications are more detailed than before
  - Incorrect statements on the application can lead to denied or reduced claim payout
- Multifactor authentication requirements
  - Applications are being denied or will have higher deductibles if MFA is not in place
- Expect a forensics visit
  - Vital as they help close the gaps that permitted the breach, but they also reveal weak controls
- One of the top 5 reasons for non-payment
  - Failing to require or complete information security training
- **Poor control environments may reduce claim payout**

FORV/S

Your Homework

- Perform risk assessments (foundation of the information security program)
- Enable Multi-factor authentication on email (It is **free** if using Office 365)
- Enforce information security training to **100%** of staff, at least annually (including management)
- Ensure network activity and endpoints are logged **and** monitored
- Use the **free** tools available to perform security self-assessments
  - HICP and NIST Cybersecurity Frameworks
- Require your security staff complete **ongoing** continuing education
  - Security risks change daily
- Management must **set the tone** for security
  - Information security **is** a management responsibility!

FORV/S

Q&A

FORVIS

A Quote to Remember!

FORVIS

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office

Thank you!

forvis.com

FORVIS

Assurance / Tax / Advisory