



American
Heart
Association.



FINANCIAL
PLANNING
ASSOCIATION

**SECURITY, DATA, AND HACKERS OH MY!
EVERYTHING YOU WANTED TO ASK ABOUT CYBERSECURITY
BUT WERE AFRAID (OR DIDN'T KNOW) TO ASK**



American Heart Association®

Professional Advisor Network



JOIN NOW



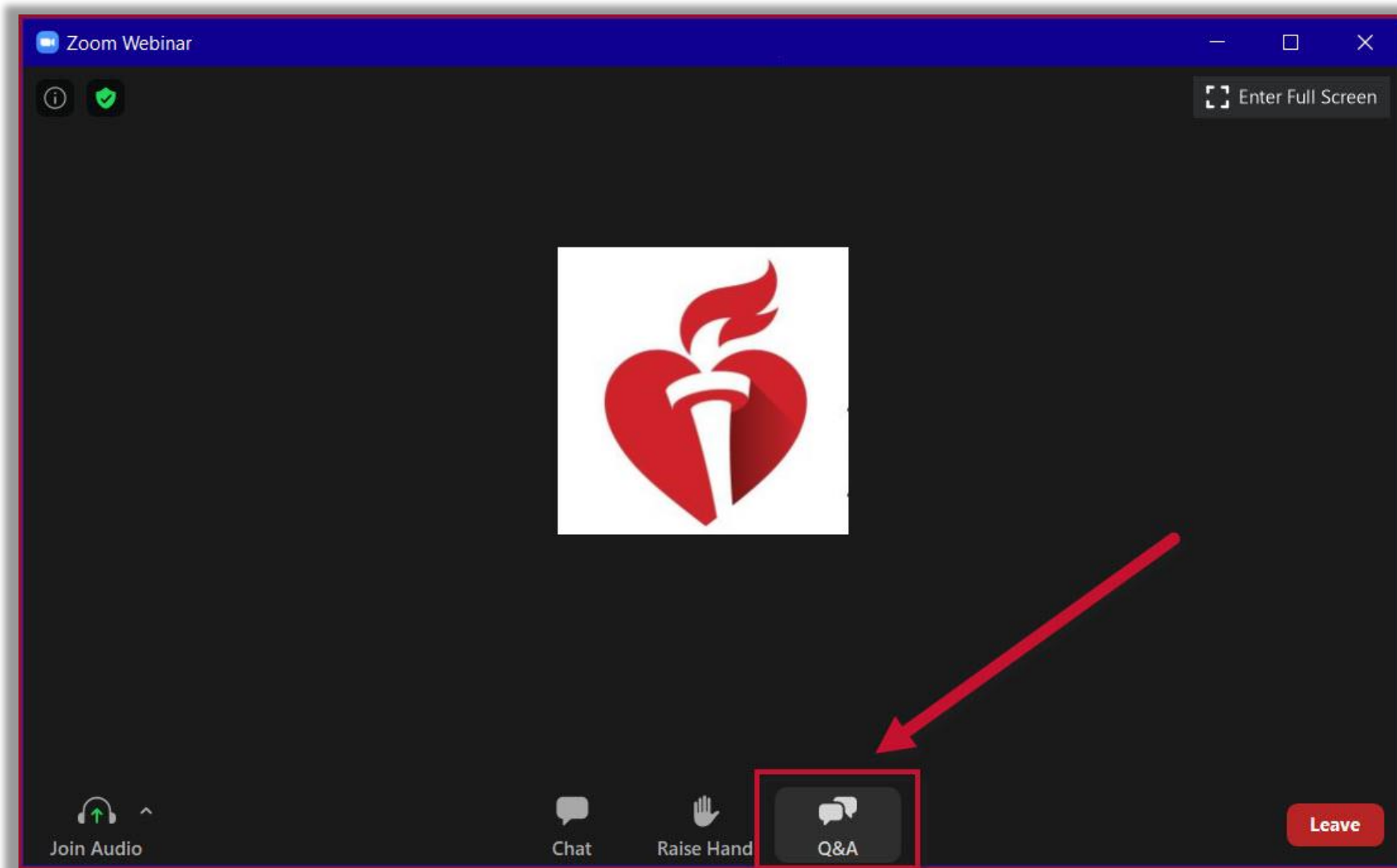
*Together, we can be a relentless force
for a world of longer, healthier lives.*

HEART.ORG/FPA



**SECURITY, DATA, AND HACKERS OH MY!
EVERYTHING YOU WANTED TO ASK ABOUT CYBERSECURITY
BUT WERE AFRAID (OR DIDN'T KNOW) TO ASK**

HOW TO ACCESS THE Q & A FEATURE



PRESENTER



Angeline Chen

General Counsel and
Chief Administrative Officer

MarkLogic Corporation

WHAT ARE WE TALKING ABOUT REALLY?

LET'S START WITH THE BASICS ...

WHAT IS CYBERSECURITY?

Protecting electronic devices and associated data and information

PROTECT FROM
CRIMINAL ACTIVITY

PROTECT FROM
INADVERTENT HARM

KEY TAKEAWAY: BE PREPARED.

WHY CYBERSECURITY MATTERS

VULNERABILITY

Small business
and law firms are
seen as easy
targets

BUSINESS COSTS

Attacks can have
significant impact on
your business by way of
costs and disruption

REPUTATION

Clients and
employees expect
and trust you to
keep their
information secure

DOING NOTHING IS A CHOICE AND CARRIES THE MOST RISK.

WHY SHOULD YOU CARE?

- ✓ Cyber incidents can be costly
- ✓ Cyber incidents can be extremely disruptive
- ✓ Clients and patients expect you to protect their data
- ✓ Numerous laws, regulations and professional standards now require basic cyber hygiene
- ✓ Threats are increasing
- ✓ Businesses and individuals are dependent on technology
- ✓ The world is hyper-connected

LEGAL AND REGULATORY REQUIREMENTS

- Notification
- Reporting
- Self-Assessments / Third-Party Assessments
- Systems and access controls
- Information security and assurance policies and procedures
- Compliance with specific standards
- Provision of credit monitoring / other services to victims
- Training

ORGANIZATION

INDUSTRY

JURISDICTION

CONTRACTUAL

“TECHNICAL COMPETENCE” REQUIREMENT FOR LAWYERS

ABA Model Rule of Professional Conduct 1.1 (Lawyers Duty of Competence), Comment 8:

- *... a lawyer should keep abreast of ... the benefits and risks associated with relevant technology ...”*

ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 477R (rev May 22, 2017):

- *Requirement to undertake reasonable efforts to prevent inadvertent or unauthorized access.*
- *Requirement to take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.*

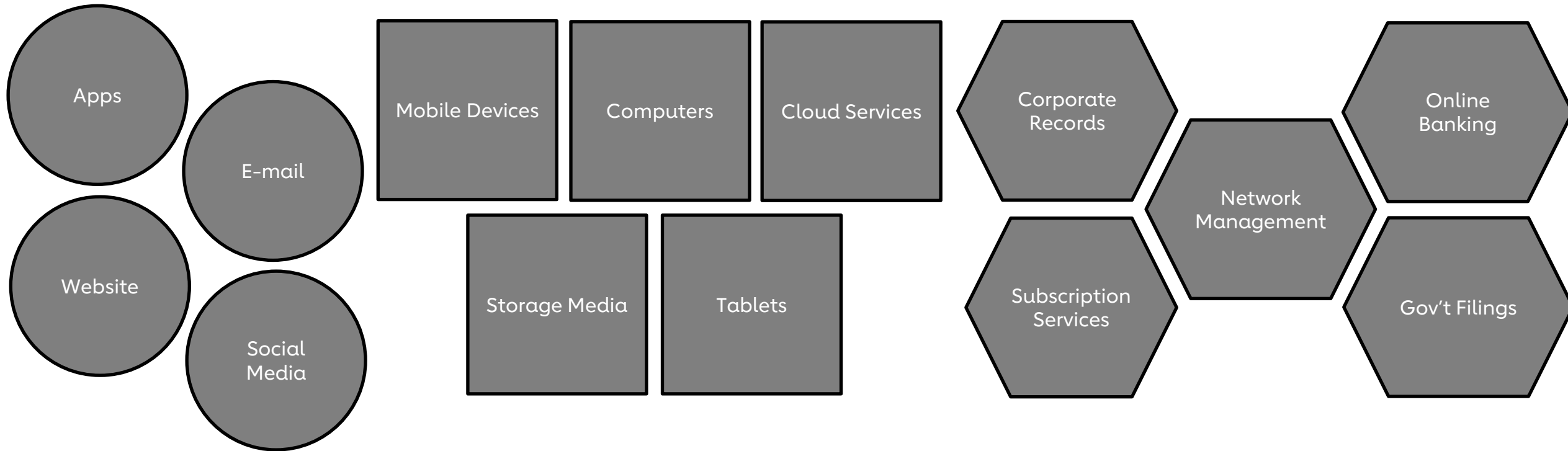
FOR THE RECORD...

What is the difference between cybersecurity and privacy?

- **CYBERSECURITY:** Safeguarding the data, the systems, and the people (including but not limited to protecting against the unauthorized access to data)
- **PRIVACY:** Safeguarding user identity and personally identifiable information

Distinguishing between these two domains can be complex and there are certainly areas of overlap between the two.

HOW DIGITAL ARE YOU?



Personal <--> Business <--> Client <--> Environmental

Do you know where your data is?

RECENT SECURITY BREACHES

COMPLIANCE WEEK

FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

Details murky in Samsung's second data breach this year

By Aaron Nicodemus | Tue, Sep 6, 2022 5:49 PM



South Korean electronics manufacturer Samsung confirmed it had lost personal data of an unspecified number of users in a breach. The company is improving its cybersecurity systems following the breach.

Uber apparently hacked by teen, employees thought it was a joke / 'I think IT would appreciate less memes while they handle the breach'

DoorDash Data Breach Exposed Some Personal Customer Data

23andMe confirms hackers stole ancestry data on 6.9 million users

@lorenzofb / 12:56 PM EST • December 4, 2023

FBI says it has 'contained' a cybersecurity incident on its network

Most of the details remain a mystery.

Phishing takes financial bite out of more victim organizations

Published Feb. 28, 2023

FishPig software breach puts up to 200,000 websites at risk

SC Staff September 15, 2022

WH Smith says employee data was illegally accessed in cyber incident

Reuters

March 2, 2023 5:51 AM EST · Updated 10 months ago

Bankruptcy Counsel Reveals FTX Assets at Risk of Cyberattacks

Nov 23 2022 · 11:25 UTC by Ibukun Ogundare · 3 min read

Mar 1, 2023 - Technology

LastPass CEO takes 'full responsibility' for security breach comms

July 17, 2023

Okta hackers stole data on all customer support users in major breach

PUBLISHED TUE, NOV 28 2023 · 10:59 PM EST
UPDATED WED, NOV 29 2023 · 12:56 PM EST

SETTING OUR BASELINE

A “cyber incident” versus a “cyber breach”

Terms can sometimes be interchangeable

Distinctions can be:

- Situational

- Regulatory

- Contractual


- Defined and set by governance frameworks or standards, or

- Industry/market driven

- Made for marketing or publicity purposes

How much is known about what is happening/happened

Degree of severity (of expected or actual impact)



Houston, we
have a
problem

DEFINITION

[Legal boilerplate language: *For purposes of this presentation ...*]

A cyber breach is an incident through which:

Confidential, sensitive, or protected information is disclosed, stolen, or taken from an information system:

Without the knowledge or authorization of the system's (or the data's) owner, and/or

To or by an unauthorized person, and or

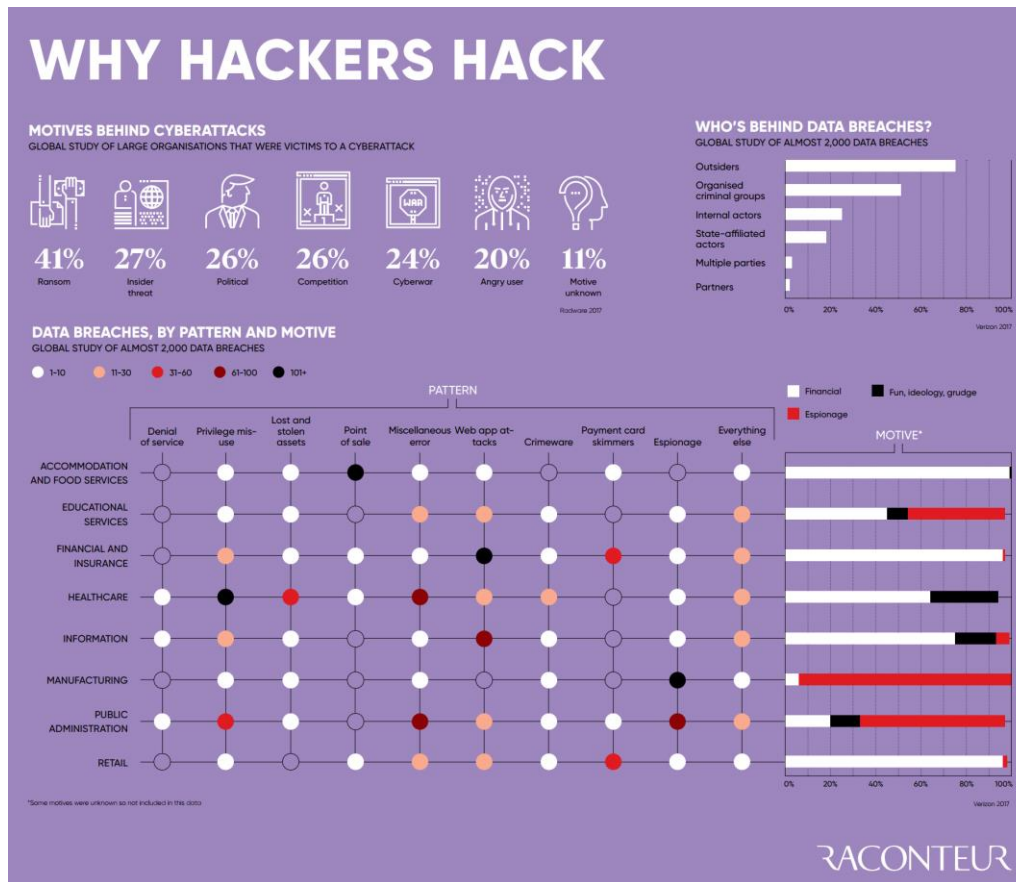
Unauthorized access to an organization's electronic digitized data, applications, networks or devices that is achieved by an intentional actor.

THE CURRENT CYBER LANDSCAPE

IMPACT OF CYBER INCIDENTS

- Global cyber attacks increased by 38% in 2022, and expected to grow by at least 15% YOY, reaching **\$10.5 trillion USD** annually by 2025.
- The average data breach cost in 2022 was **\$4.35 million** (an increase of 2.6% year-over-year from 2021). The U.S. continues to have the highest cost of a data breach at **\$5.9 million**.
- Organizations working from remote paid an average of almost \$1M more than organizations that did not utilize a remote working model
- Healthcare had the highest data breach costs of any industry for the twelfth consecutive year (paying an average of \$10M for a data breach)
- Ransomware continued its upward trend, increasing nearly 13%
- 61% of small and medium size businesses (SMBs) were targets in 2021
- Employees of SMBs experience 350% more social engineering attacks than those at larger organizations.

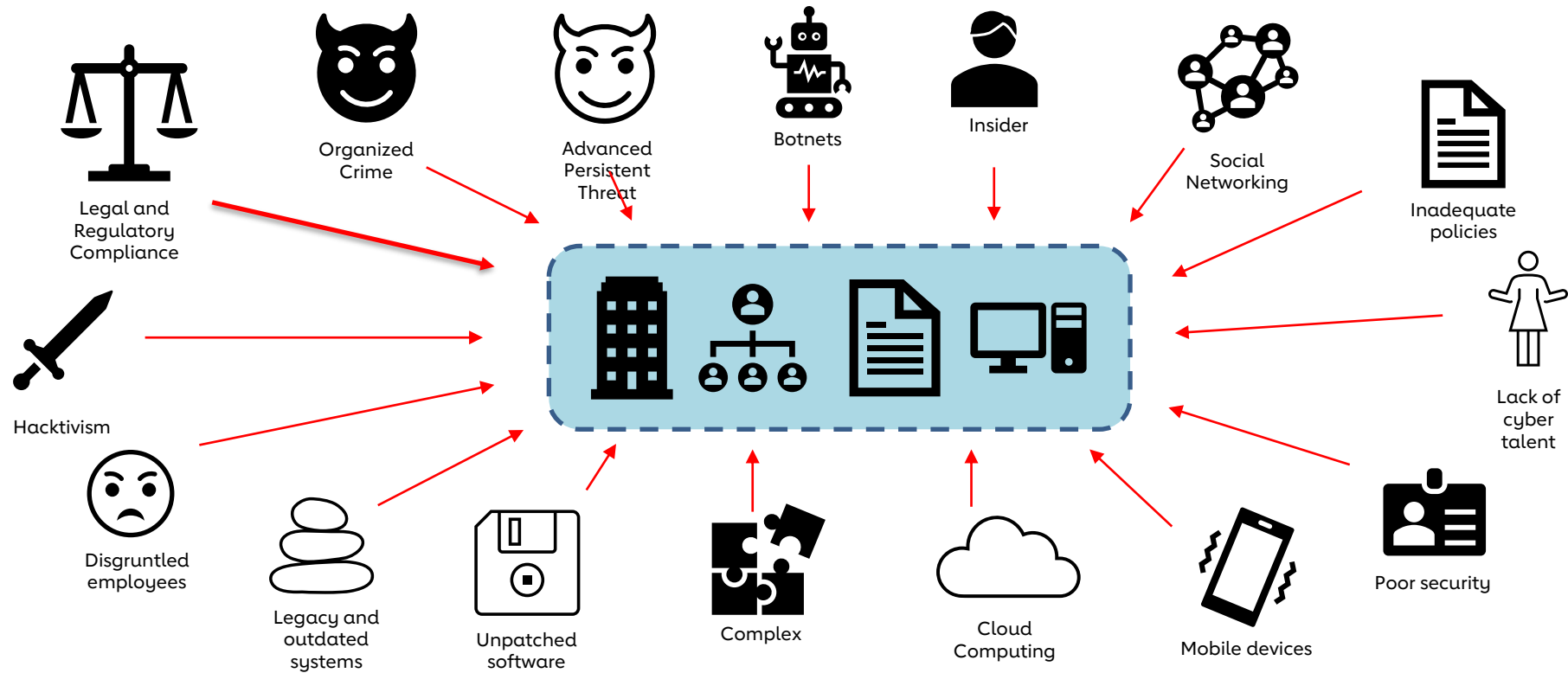
WHY HACKERS HACK



- Financial gain
- Corporate espionage/theft
- Notoriety and bragging rights
- Revenge
- Vandalism
- Political reasons
- Curiosity
- Boredom
- Challenge

<https://www.raconteur.net/infographics/why-hackers-hack/>

THREAT/ATTACK VECTORS



WHAT ARE THE THREAT ACTORS AFTER?

TLDR: EVERYTHING

HIGH VALUE DATA

- Personally Identifiable Information
- IP / Trade Secrets
- Financial Information
- Protected Health Information
- Passwords

LEVERAGE AND EXPLOITATION

- Financial Gain
- Business Disruption
- Corporate Espionage
- Sabotage/Vandalism/Nuisance
- Hacker/group reputation
- Organized Crime
- Blackmail/Extortion

MOST COMMON FORMS OF ATTACK

- Malware
- **Phishing**
- **Business E-mail Compromise**
- **Ransomware**
- Spoofing
- Distributed Denial-of-Service (DoS) Attacks
- Identity-Based Attacks
- Code Injection Attacks
- Supply Chain / Service Provider Attacks
- Insider Threats

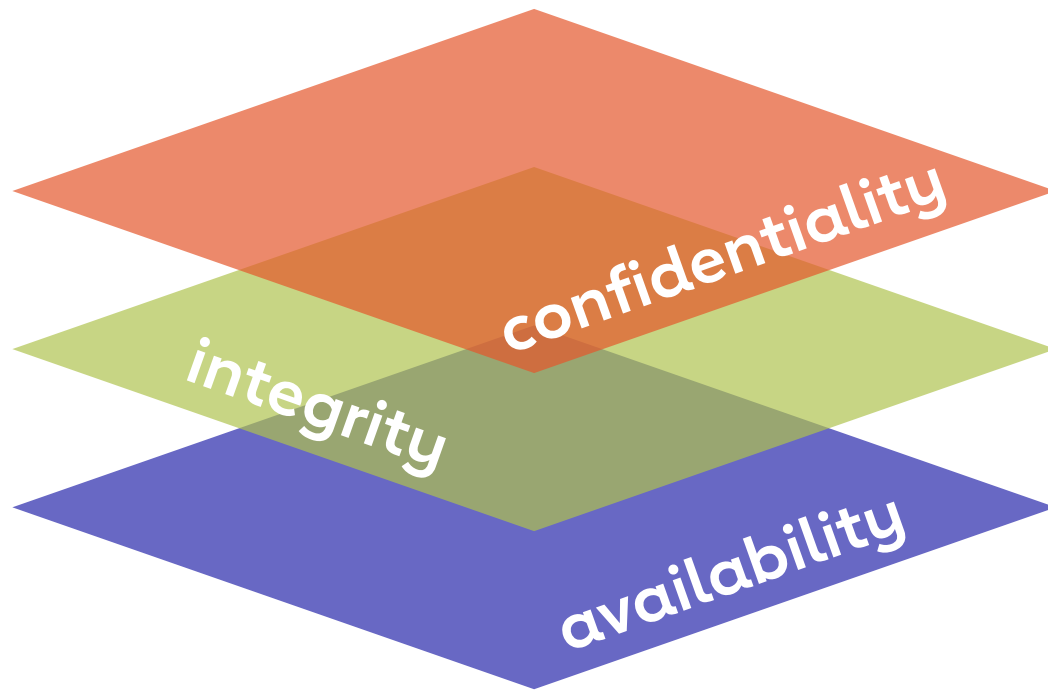
Tactics, Techniques, and Procedures (TTP)

Tactic – highest-level description of threat actor behavior

Technique – more detailed description of behavior in context of a tactic

Procedure – lower-level, highly detailed description of the behavior in the context of a technique

CYBERSECURITY OBJECTIVES: THE CIA TRIAD

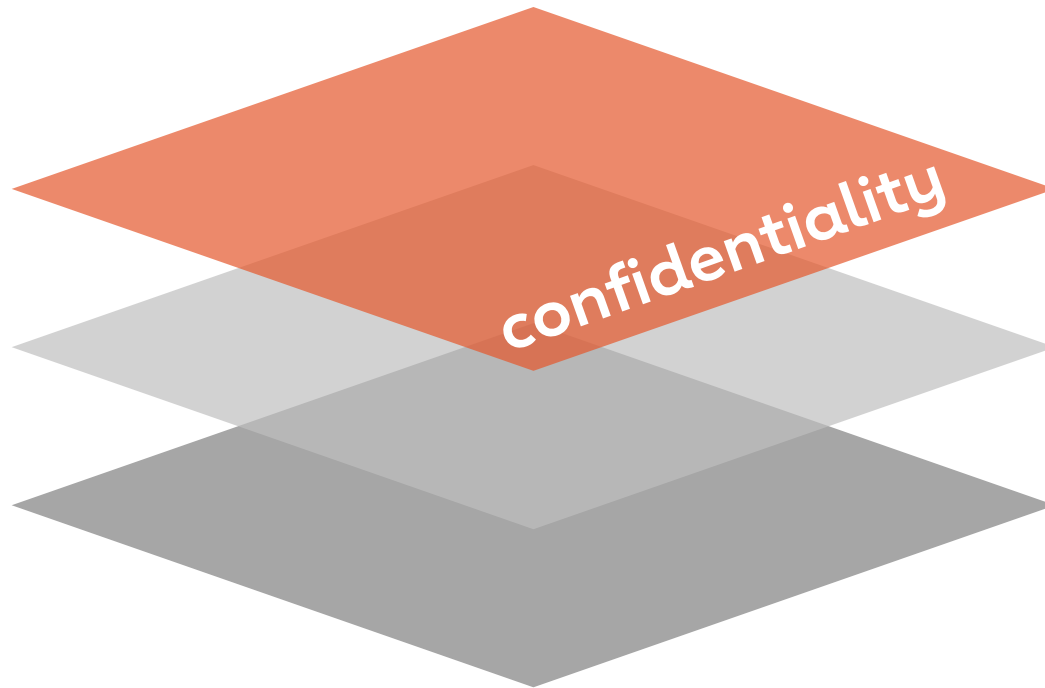


CONFIDENTIALITY: Protecting information from unauthorized access and disclosure

INTEGRITY: Protecting information from unauthorized modification or destruction

AVAILABILITY: Assuring that information is available to authorized users when needed

THE CIA TRIAD: CONFIDENTIALITY

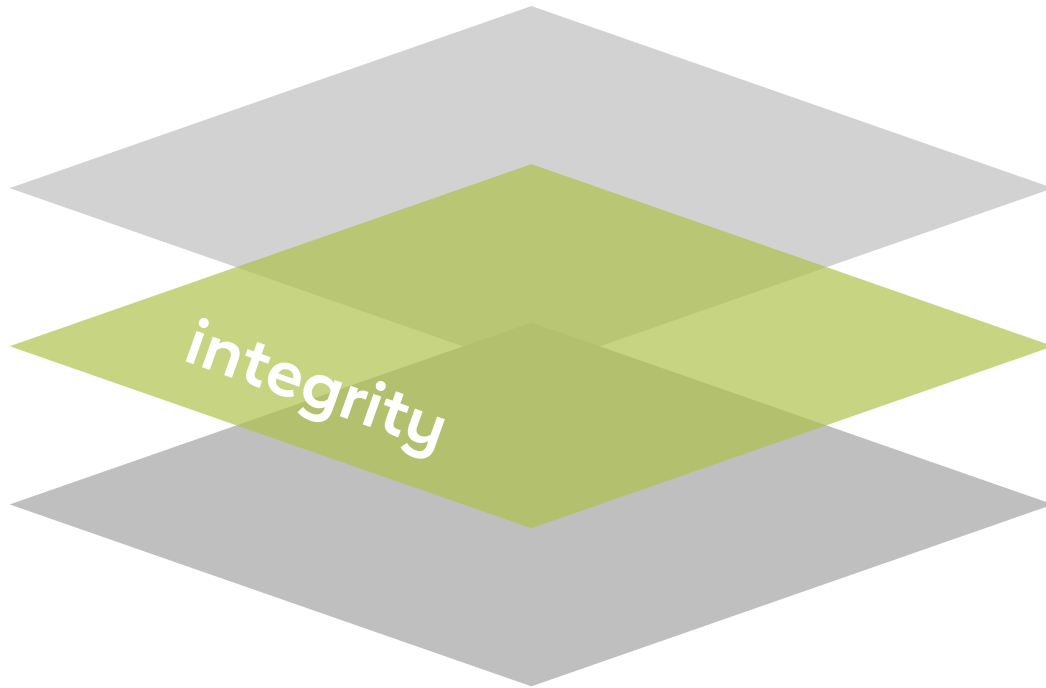


CONFIDENTIALITY: Protecting information from unauthorized access and disclosure

Examples:

- Unauthorized access to client data
- Employee e-mail account compromise
- Theft or loss of mobile device
- Ransomware and exfiltration of data

THE CIA TRIAD: INTEGRITY



INTEGRITY: Protecting information from unauthorized modification or destruction

Examples:

- Unauthorized changes to data
- Ransomware attack
- Insider threats
- Website Defacement

THE CIA TRIAD: AVAILABILITY



AVAILABILITY: Assuring that information is available to authorized users when needed

Examples:

- DDoS Attack
- IT equipment failure
- Malware infections
- Power or service disruption
- Insider threat

PHISHING

Definition: A cyber attack technique used to acquire sensitive data through fraudulent solicitation and tricking users by masquerading as a reputable entity or person.

- Uses any form of digital communication (e.g., e-mail, website or text). Utilizes a range of techniques such as spoofing, social engineering, spear phishing, malware, smishing, and vishing. Includes imposter scams.

THREAT INDICATORS

- *Suspicious or unusual sender*
- *Poor grammar and spelling*
- *Urgency of request*
- *Links or attachments*
- *Requests for sensitive info*

BE A HARDER TARGET

- *Verify senders / callers*
- *Don't share personal info*
- *Use anti-phishing software*
- *Use multi-factor authentication*
- *Keep software up-to-date*
- *Educate employees*

BUSINESS E-MAIL COMPROMISE (BEC)

Definition: *A specific type of targeted phishing (spear fishing) with the objective of tricking authorized users into taking harmful actions.*

- Typically uses e-mail. Utilizes different techniques such as spoofing, social engineering, account compromise, payment diversion.

THREAT INDICATORS

- *Be suspicious!*
- *Be observant.*
- *Trust but verify.*
- *Check the sender.*
- *Check the quality.*

BE A HARDER TARGET

- *Review your privacy settings.*
- *Flag or block e-mails.*
- *Set expectations for employees, clients and external recipients.*

BEC KEY VULNERABILITIES

- Human nature
- Lack of documented policies and procedures on how payments must be authorized and executed
- Lack of reinforcement and monitoring of those policies and procedures
- Lack of employee and service provider awareness and training
- Lack of multi-factor authentication and proactive phishing defensive measures (people and systems)

RESPONDING TO A BEC

- Immediately attempt to stop or recall the transfer
- Immediately notify financial institutions involved
- Immediately contact law enforcement in the relevant jurisdictions
 - Victims may need local counsel in the relevant jurisdictions
 - *Under FinCEN's Rapid Response Program, US law enforcement can issue a request to overseas banks to recall the funds if they are notified within 72 hours*
- Determine the nature of the compromise
 - If your network is involved, consult internal and external counsel and infosec personnel immediately.

RANSOMWARE

Definition: *Malware that prevents you from accessing your computer files, systems, or networks, and demands that you pay a ransom for their return or release.*

- Typically uses system or network attacks or e-mail compromise. Utilizes different techniques such as phishing, malvertising, exploit kits and remote desktop or system protocol attacks.

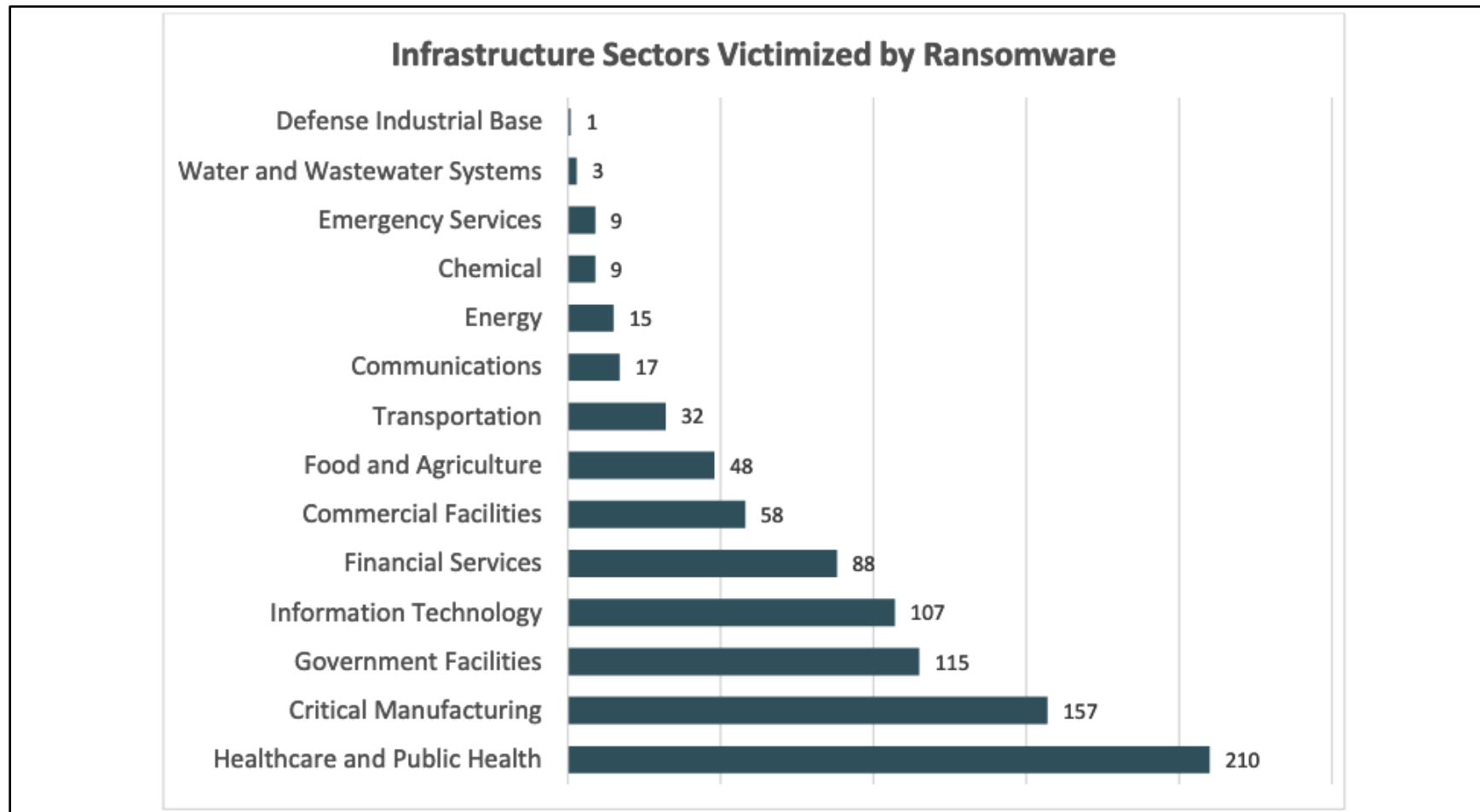
THREAT INDICATORS

- *Suspicious network traffic*
- *Unusual or new files with unknown extensions*
- *Unauthorized access attempts*
- *System impairment*

BE A HARDER TARGET

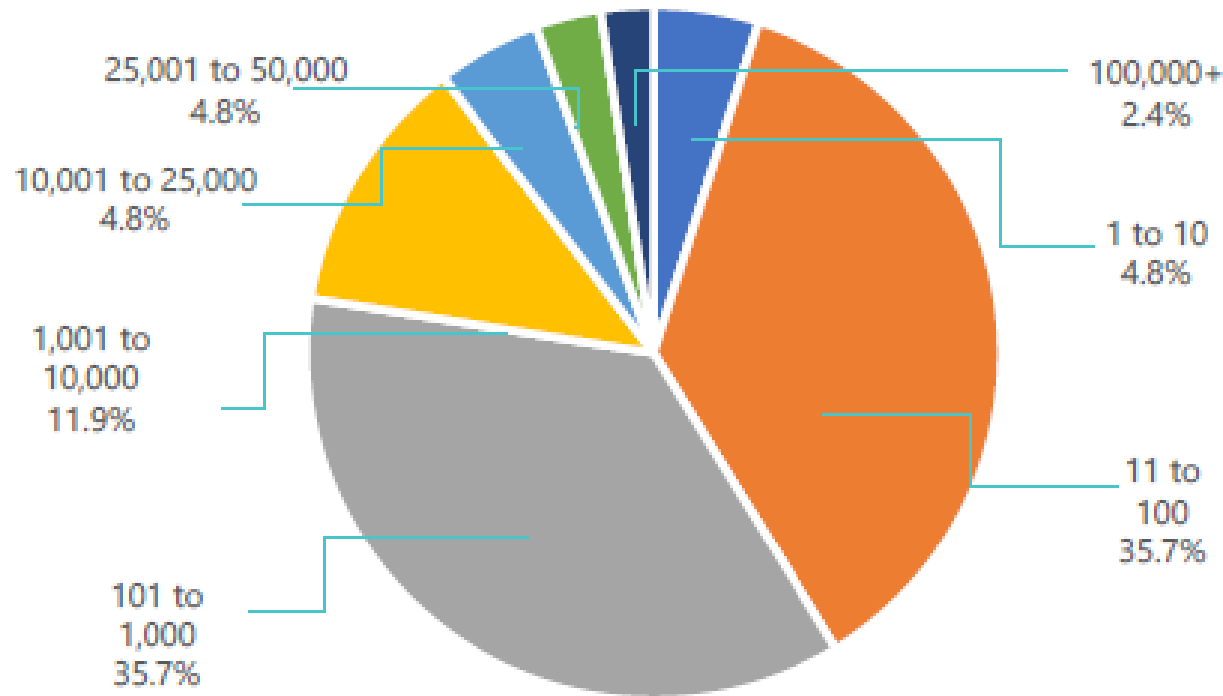
- *Regular back-ups*
- *Anti-virus software*
- *User training*
- *Regular software updating*
- *Multi-factor authentication*

CRITICAL INFRASTRUCTURE RANSOMWARE ATTACKS (2022)



RANSOMWARE ATTACK TARGETING

Number of Employees



- Nearly ½ of ransomware attacks take place in mid-size entities between 1K and 10K employees
- Small to mid-size entities typically have lower cybersecurity maturity
- Large enterprises are not immune – software vulnerability attacks leave them exposed as well

RANSOMWARE COMMON INFECTION METHODS

- E-mail
 - Script files (can be embedded)
 - Social engineering
 - Links to malicious files on share sites
- Infected Websites
 - Exploit toolkits
 - Malvertisement
- Targeted attacks
 - Server exploitation
 - Stolen credentials

RESPONDING TO A RANSOMWARE ATTACK

- Immediately identify and isolate your impacted systems
- GATHER INCIDENT RESPONSE TEAM
- Immediately contact internal and external counsel
- Immediately notify law enforcement in the relevant jurisdictions
 - Report the event and request assistance
- Perform thorough investigation (including eradication of malware)
- Execute remediation and recovery plans

DOCUMENT / CONTACT INSURANCE CARRIER / COMMUNICATE TO EMPLOYEES

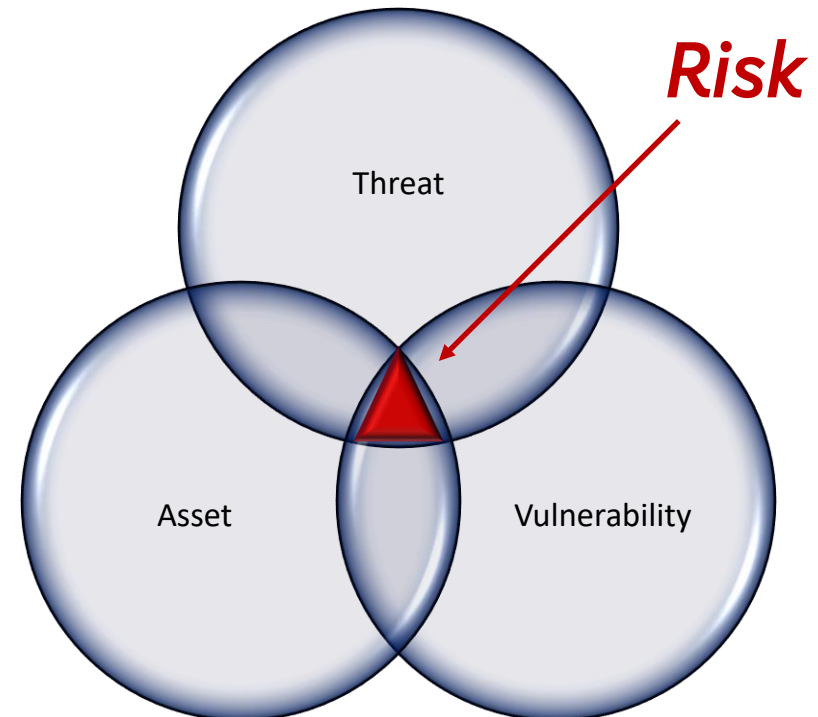
LET'S TALK ABOUT MANAGING YOUR RISKS

ELEMENTS OF CYBERSECURITY RISK

- What are the **THREATS**?
- What are the **VULNERABILITIES**?
- What is the **LIKELIHOOD** of a threat exploiting a vulnerability?
- What would be the **IMPACT** of this to you and your business?

WHAT ARE YOU PROTECTING?

1. Identify your business assets
2. Identify the value of those assets
3. Document the impact to your business in the event of loss or damage of those assets
4. Identify the *likelihood* of that loss or harm occurring
5. Prioritize your mitigation actions accordingly



SPECIAL CONSIDERATIONS IN ESTATE PLANNING

Many clients now have digital assets. These digital assets may have sentimental and/or financial value.

Sentimental Value

- Digital photos and videos
- E-books
- Music
- Social media accounts
- Subscriptions

Financial Value

- Cryptocurrency
- Bank and investment accounts
- NFTs or other digital IP
- Influencer accounts or blogs
- Income-generating digital content

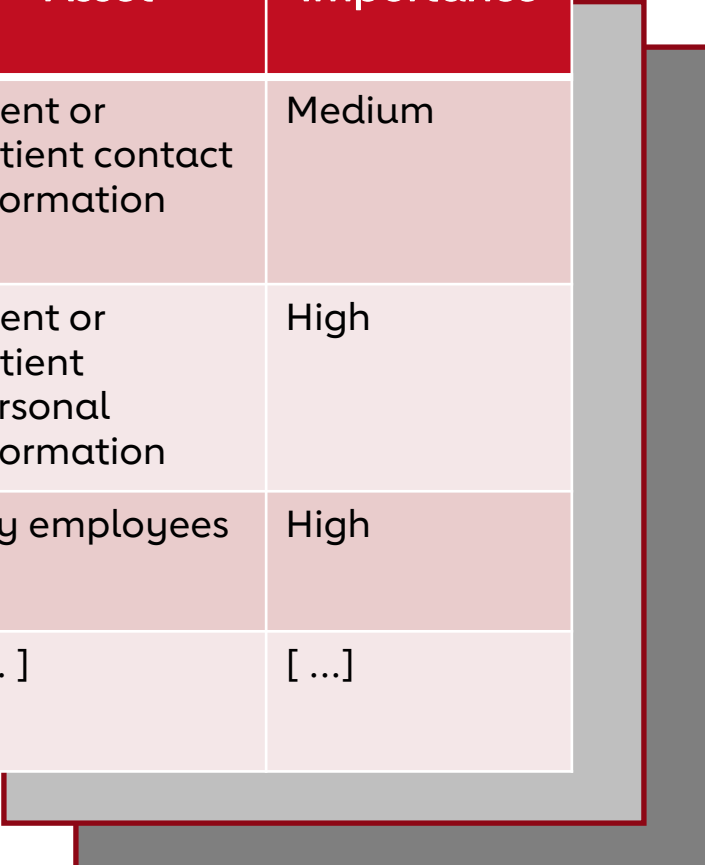
Often it is a challenge to collect digital assets in the event of a client's death or incapacity.

1. IDENTIFYING YOUR BUSINESS ASSETS

Types of Information

- Client or Patient Information
- Key employees (talent)
- Business information
- Banking Information
- Business partners
- Equipment & facilities
- Critical business processes

Asset	Importance
Client or patient contact information	Medium
Client or patient personal information	High
Key employees	High
[...]	[...]



2. VALUATE YOUR ASSETS

Go through your
asset list and for
each one ask
questions:

- What would happen if this info was made public or released to unauthorized persons?
- What would happen if this information was inaccurate or unreliable?
- What would happen if this asset couldn't be accessed or used?

3. EVALUATE AND DOCUMENT POTENTIAL LOSS OR DAMAGE

- Consider and determine (or estimate) the impact to you and your business if an asset was lost, damaged, or otherwise reduced in value
- *Note: this impact and the assigned value may be different from the importance you ascribed to it in Steps 1 and 2*

Asset	Value of Asset	Impact of Loss or Damage
Client or patient contact information	Medium	Low (can make back-ups in case of loss)
Client or patient personal information	High, due to regulations and professional ethics	High
[...]	[...]	[...]

4. IDENTIFY THE LIKELIHOOD OF LOSS OR DAMAGE

- Consider and list the threats to each asset
- Evaluate the probability that loss or damage to the asset may occur due to the identified threat(s)
- *Reasonable estimates are fine and different methodologies can be used*

Asset	Value of Asset	Impact of Loss or Damage	Threat to Asset	Likelihood of Threat Occurring
Client or patient contact Info	Medium	Low (can make back-ups in case of loss)	Hackers, ransomware, insider threat	Medium
Client or patient information	High, due to regulations and professional ethics	High	Hackers, ransomware, phishing	High
[...]	[...]	[...]	[...]	[...]

5. IDENTIFY PRIORITIES AND POTENTIAL SOLUTIONS

- Review your impact and likelihood scores to identify priorities.
- Identify potential solutions.
- *Develop a plan (including funding and timelines) to implement the solutions.*

SAMPLE PRIORITY STRUCTURE

High: Implement an immediate solution

Medium: Schedule a near-term solution

Low: Schedule a solution or monitor

“TOP TEN” TIPS

- Be careful of unexpected e-mails or e-mails from unknown senders, attachments and embedded web links, and voice calls from unknown numbers.
- **Do not click on a link or open attachments you were not expecting – *(don't trust, and always verify.***
- Do not download software from unknown web pages or QR codes.
- Perform back-ups and update software regularly.
- Refresh equipment and devices
- Use VPNs and multi-factor authentication.
- Encrypt documents (to and from clients, and in storage)
- ***Never give out your username or password.***
- Establish and train employees on policies on Internet and device usage.
- Adopt a “security mindset.”

SOURCES AND REFERENCES:

American Bar Association Cybersecurity Handbook

https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/201801/cybersecurity_handbook/

American Bar Association Formal Opinion 477R, "Securing Communication of Protected Client Information" (May 11, 2017), located at

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf

American Medical Association web page on physician cybersecurity (May 26, 2022), located at <https://www.ama-assn.org/practice-management/sustainability/physician-cybersecurity>

NIST Special Publication 800-12, Rev. 1: *An introduction to information Security*, located at <https://doi.org/10.6028/NIST.SP.800-12r1>

NIST Special Publication 800-30, Rev. 1: *Guide for Conducting Risk Assessments*, located at <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>

QUESTIONS





**SECURITY, DATA, AND HACKERS OH MY!
EVERYTHING YOU WANTED TO ASK ABOUT CYBERSECURITY
BUT WERE AFRAID (OR DIDN'T KNOW) TO ASK**

THANK YOU!



JOIN NOW

Join the AHA Professional Advisor Network:

[Heart.org/fpa](https://heart.org/fpa)

Find an AHA Representative in your Area:

[Heart.org/advisor](https://heart.org/advisor)

Join the Financial Planning Association:

JoinFPA.org

Contact Us: Advisor@heart.org | 888-227-5242

YOUR NEXT STEPS

To receive credit, navigate to the FPA Learning Center and follow these steps:

- Login to your FPA profile
- Click on 'Dashboard' on left side of page
- Find this session and click on the title
- Complete the 'Course Evaluation' and submit
- Then you can view/print your certificate of completion, confirming your CE credit will be reported

Download Resources & Slides (Optional)

- Slides and resources are available to you within Learning Center