

Cybersecurity: *Risks and Mitigations*



Rehmann
EMPOWER YOUR PURPOSE®

Presenter



Paul Kennedy

Senior Manager | CISSP | CISA | vCISO
616.301.6318 | paul.kennedy@rehmann.com

- Virtual chief information security officer (vCISO)
- Leads Rehmann's IT Audit and Assessment team
- Advises clients in a variety of industries to implement, monitor and improve their security controls.
- Leads cyber security consulting engagements such as:
 - Security strategy development
 - Vulnerability and penetration testing
 - Social engineering testing
 - Information security training
- Certified Information Systems Security Professional (CISSP)



Headlines and Trends

Have you seen the headlines?

ValleyCentral.com

Russian ransomware gang hacks BPUB

BROWNSVILLE, Texas (ValleyCentral) – On Monday, a cyber security firm reported a Russian ransomware gang hacked the Brownsville Public...

1 day ago




Bleeping Computer

FBI: Ransomware gang breached 52 US critical infrastructure orgs

The US Federal Bureau of Investigation (FBI) says the Ragnar Locker ransomware group has breached the networks of at least 52 organizations...

2 days ago




Dark Reading

FBI Alert: Ransomware Attacks Hit Critical Infrastructure Organizations

Bureau releases indicators of compromise for the RagnarLocker ransomware that has hit 10 different critical infrastructure sectors.


15 hours ago



Los Angeles Times

Hackers release data after LAUSD refuses to pay ransom

9 days ago




Threatpost

Samsung Confirms Lapsus\$ Ransomware Hit, Source Code Leak

The move comes just a week after GPU-maker NVIDIA was hit by Lapsus\$ and every employee credential was leaked.

2 days ago




StateScoop

K-12 cyber incidents are drastically undercounted, group says

The number of ransomware attacks, data breaches and other cyber incidents affecting K-12 schools could be 10 to 20 times greater than what's...


3 hours ago



Bloomberg Law

Cyberattack on Suffolk County, NY May Be Costly, Fitch Says

5 days ago




Nextgov

CISA Warns of Ransomware Gang, Issues Indicators of ...

Processes spurring from the Ragnar Locker Ransomware have affected at least 52 critical infrastructure victims since January...

1 day ago




Education Week

Are Schools Now a Step Ahead of Cybercriminals? Not Quite ...

Publicly reported ransomware attacks against K-12 schools and districts increased last year, even as documented cyberattacks in the K-12...

3 hours ago



Why Do They Do It?



Then everything else...



Thrills



Idealism



Nation State



Hacktivism

Suffolk County, NY



The County with 1.5 million constituents shut down on Sept. 8th due to a ransomware attack.

County 911 services operated in an emergency model delegating dispatching to other counties for 2 weeks.

The attack impacted the ability of Sheriff Deputies to write tickets and enter traffic stops into county systems.

Title search services were unavailable for 4 weeks.

As of mid-October, the county had missed over \$140 Million in vendor payments and still was manually signing all payment checks.

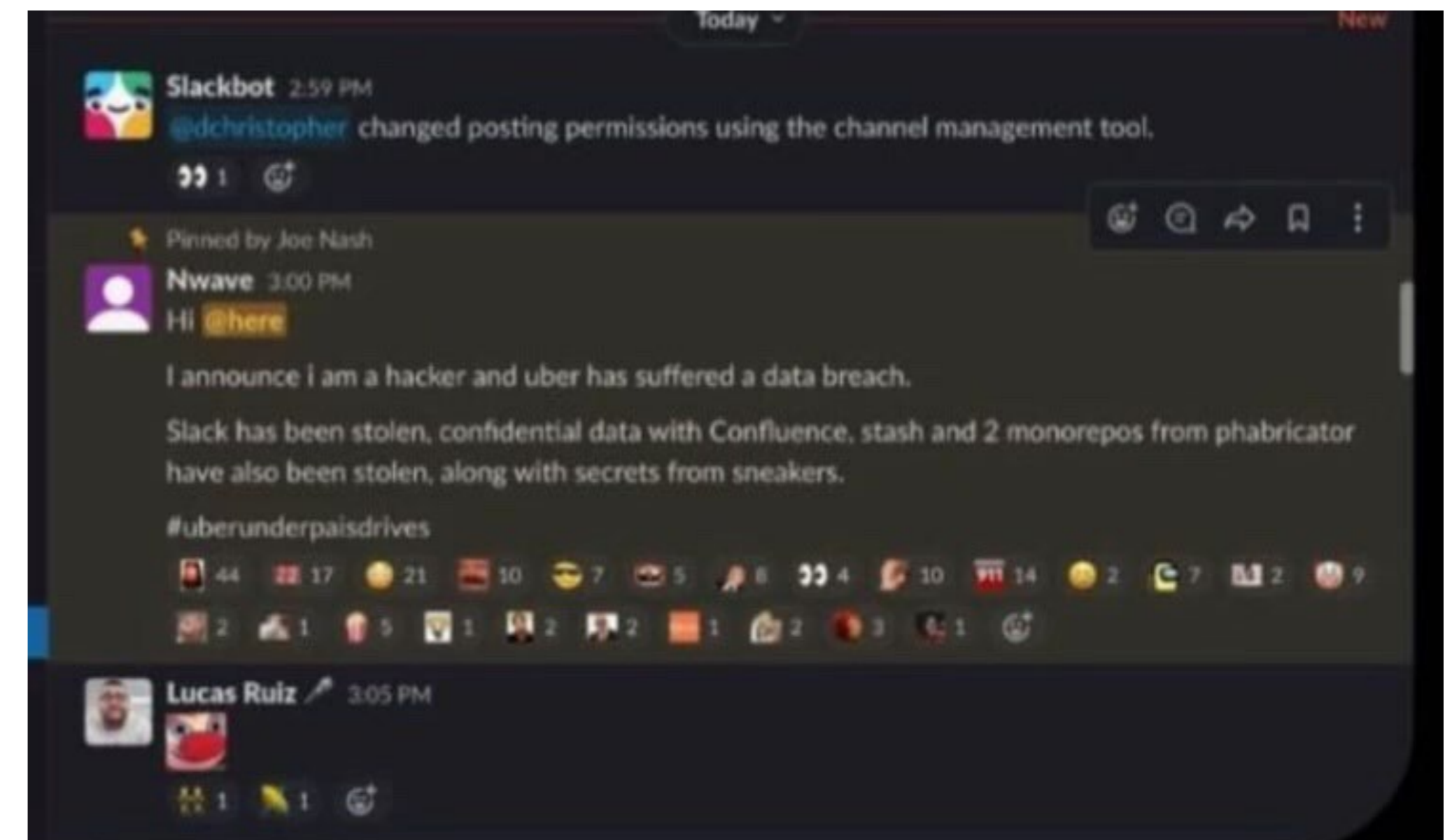
Uber



An 18 year old hacker reportedly breached the vast majority of Uber's systems.

Uber was breached despite using multifactor authentication to secure its systems.

The attacker repeatedly sent notifications to the users phone until they accepted the authentication requests.



Ponemon Institute: 2022 Cost of a Breach



Global Averages

Average total cost of a data breach

\$4.35M

Average total cost of a ransomware attack

\$4.54M

Highest country average cost (\$9.05 million)

United States

Average size of a data breach

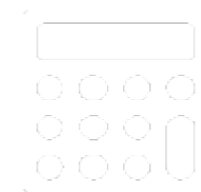
26,335 records

Time to identify and contain a breach

277 days

Highest industry average cost (\$10.10 million)

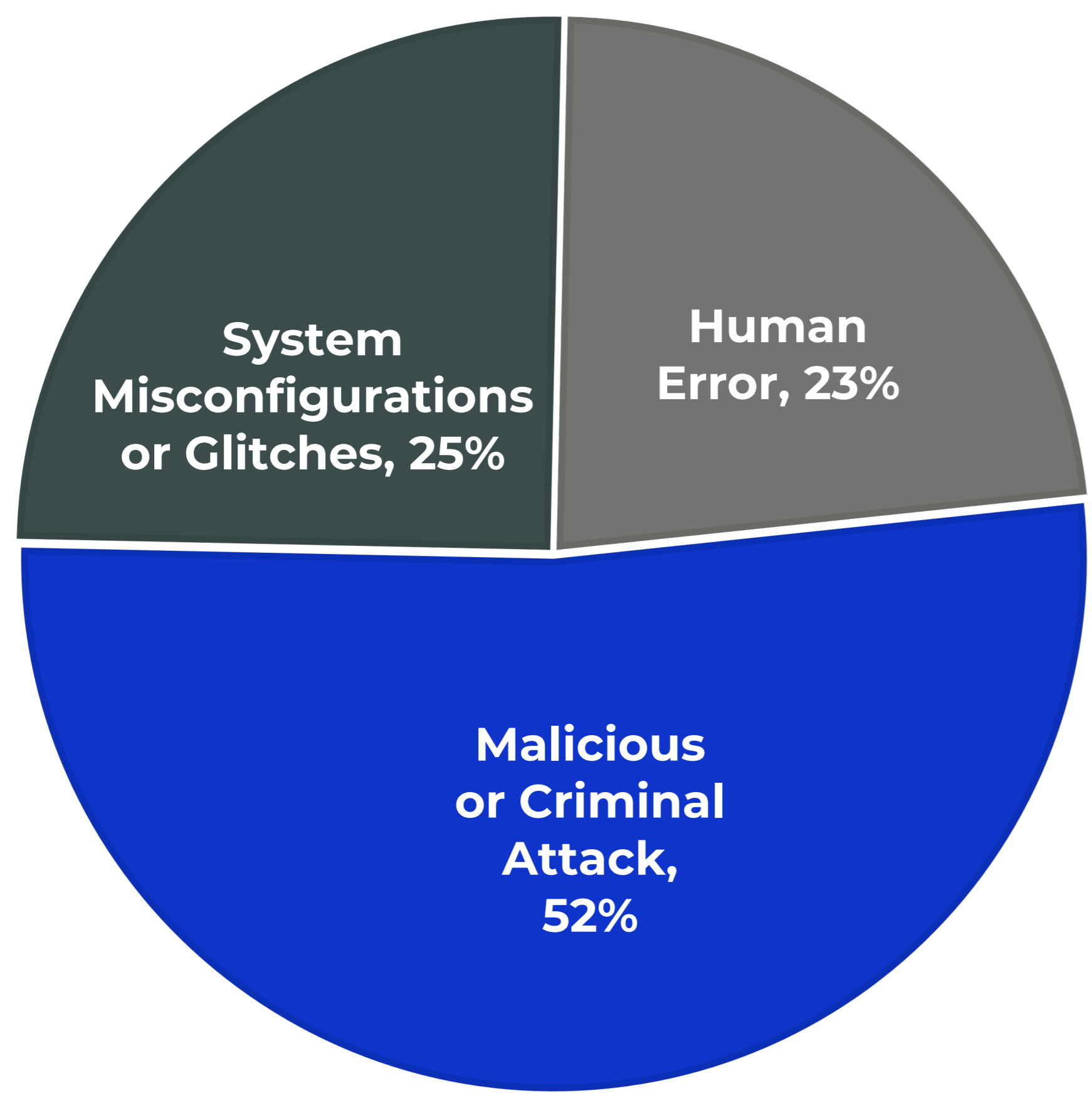
Healthcare



Long-term Impact

On average, only 53 percent of breach costs came in the first year, 31 percent accrued in the second year after a breach, and 16 percent of costs occurred more than two years after a breach.

Ponemon – Data Breach Root Causes

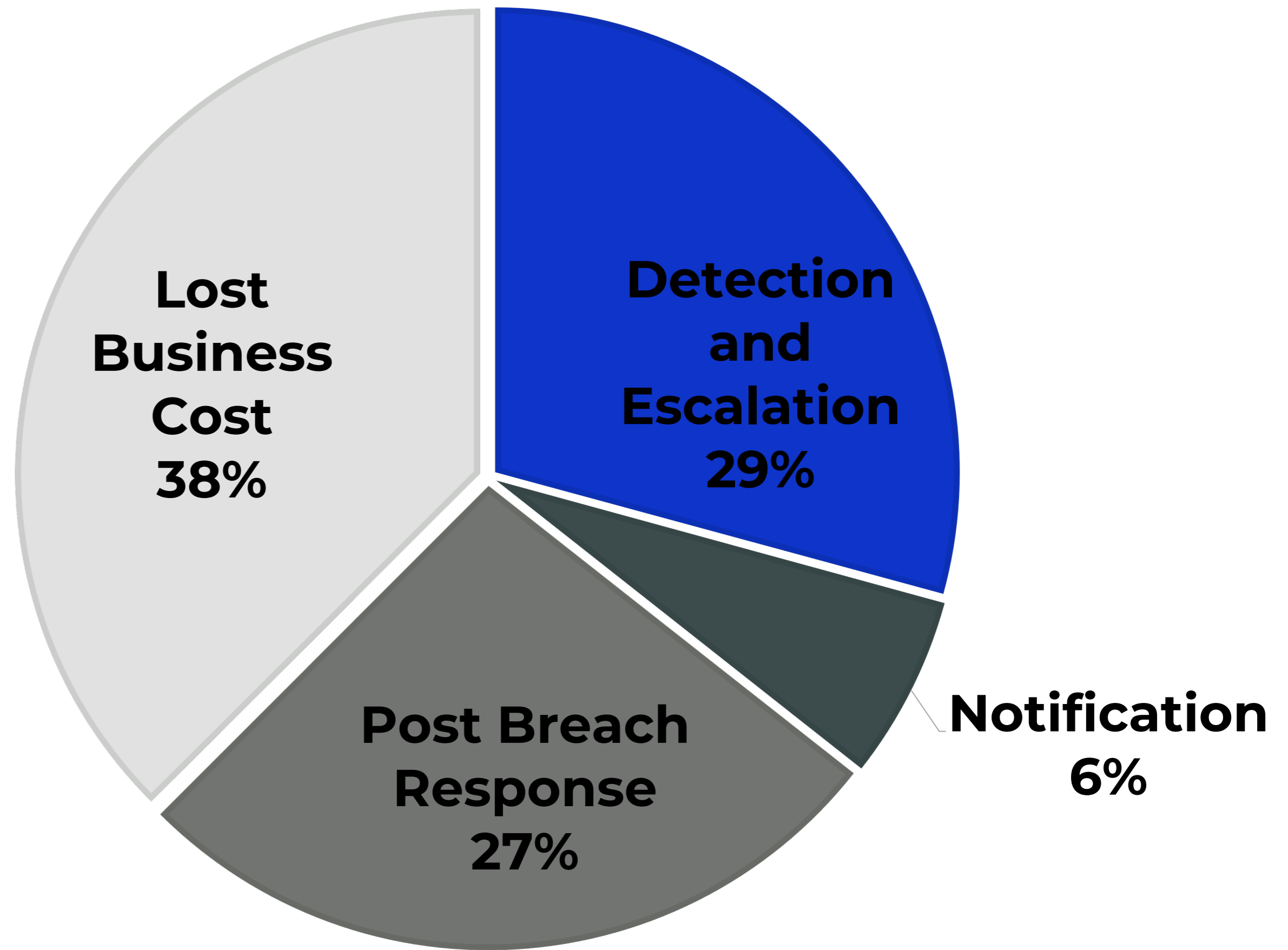


Hostile attackers are a real threat, but close to 50% of breaches were caused by the organization's personnel or systems.

Ponemon – Breakdown of Breach Costs

SMB Cost Disadvantage

It was observed that significant variation in total data breach costs by organizational size exist as smaller organizations have higher costs relative to their size than larger organizations, which can hamper their ability to recover financially from the incident.



Potential Exposure Estimates

The simple calculations to determine potential exposure:

$$\begin{aligned}
 &\text{Days of Downtime} \times \text{Cost per day of downtime} = \text{Exposure} \\
 &15 \text{ business days} \times \$3,850 / \text{day} = \$57,750 + \text{Response Costs} \\
 &\qquad\qquad\qquad \text{\$1M Annual Revenue Consultancy}
 \end{aligned}$$

$$\begin{aligned}
 &\text{Days of Downtime} \times \text{Cost per day of downtime} = \text{Exposure} \\
 &15 \text{ business days} \times \$100,000 / \text{day} = \$1,500,000 \\
 &\qquad\qquad\qquad \text{\$25M Annual Revenue Manufacturer}
 \end{aligned}$$

$$\begin{aligned}
 &\text{Number of Records with PII} \times \text{Cost per record by industry} = \text{Exposure} \\
 &2,300 \text{ patients} \times \$470 / \text{record (Healthcare)} = \$1,081,000 \\
 &\qquad\qquad\qquad \text{Average Primary Care Physician}
 \end{aligned}$$

Personally Identifiable Information (PII)



Cybersecurity for Your Clients



Attractive Targets

Significant Return on Investment

High net worth individuals (HNWIs) simply have more assets. This makes it more likely that an attacker is going to get a significant return on their time investment.

Publicly Available Information

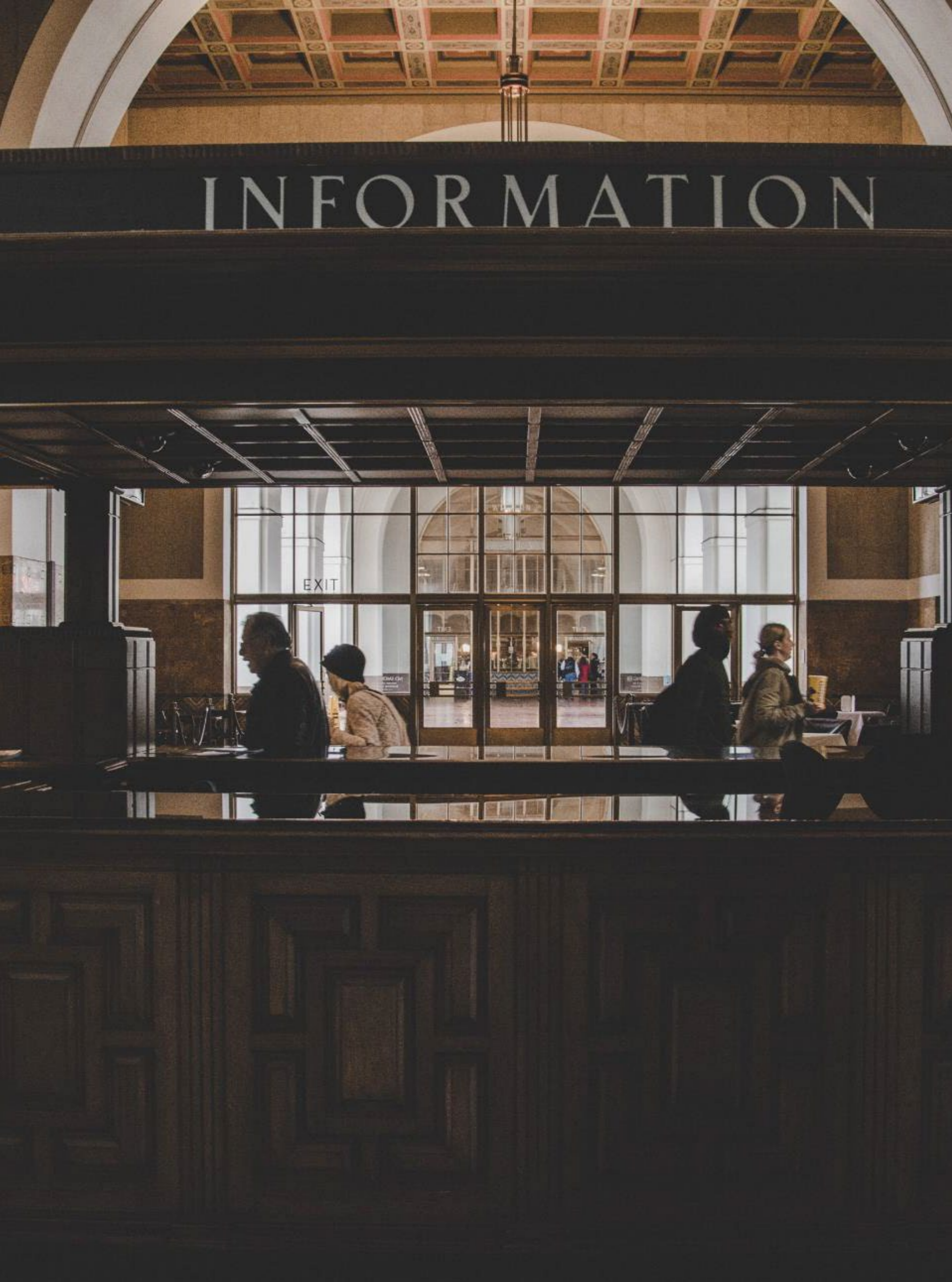
HNWIs often have significant public presences either through a company or through community engagement.

Expansive Networks

HNWIs generally are connected individuals whose relationships can be leveraged to compromise other HNWIs.

Attackers Prey on Relationships

Attackers will try to convey a sense of urgency which is all that much easier to do when a HNWI has other individuals working for them.



Open Source Intelligence (OSInt)

I picked a random executive from a Michigan based insurance company as a target. With 90 minutes of gathering publicly available information, I identified...

REDACTED

Summary – It is easy for attackers to find lots of information about us online.



Deepfakes will be the next frontier for enterprise fraud

Artificial Intelligence (AI) technology is being used to create highly believable counterfeits (in image, video, or audio format).

News of cybercriminals using an AI-generated voice in social engineering surfaced in 2019. An energy company was reportedly defrauded of US \$243,000 by scammers who used AI to mimic the voice of the firm's CEO.

In 2020, a bank in Honk Kong was defrauded of US \$35 million by attackers who used business email compromise and deepfakes to authorize the transfer.

Source: The New Norm: Trend Micro Security Predictions for 2020,

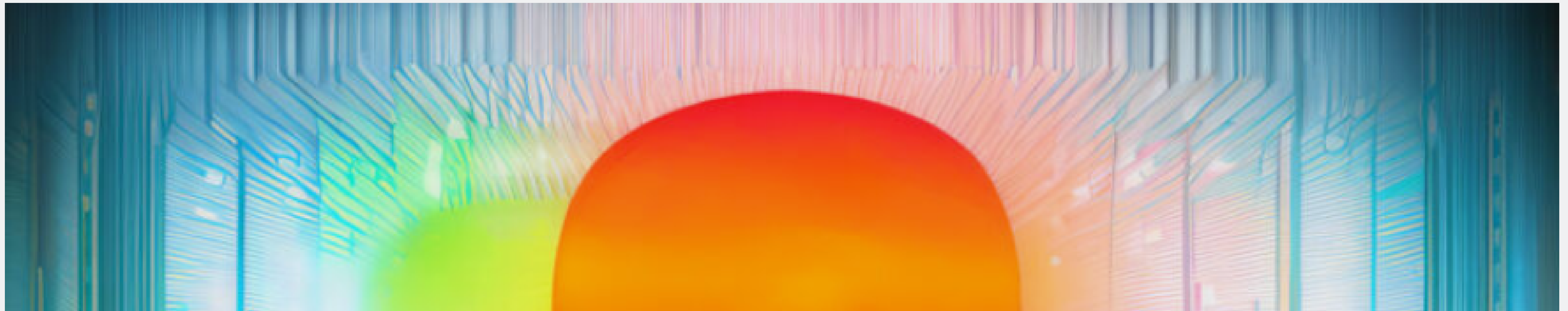
[Forbes](#)

MY VOICE IS NO LONGER MY PASSWORD —

Microsoft's new AI can simulate anyone's voice with 3 seconds of audio

Text-to-speech model can preserve speaker's emotional tone and acoustic environment.

BENJ EDWARDS - 1/9/2023, 5:15 PM



Which is a more secure password?

“i^vs6vFa”

“lance goes stagnant cane”

Which is a more secure password?

“i^vs6vFa”

0.5 to 8 hours to crack with current technology.

“lance goes stagnant cane”

1.1 quadrillion years to crack with current technology.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



› Learn about our methodology at hivesystems.io/password

Security Best Practices for Individuals

For Your Client

- 1. Password Vaults with passphrases (humans) and randomly generated long passwords (computers)**
- 2. Multifactor Authentication on everything**
- 3. Keep systems and passwords up to date**
- 4. Be highly skeptical of text or other inbound messages**
- 5. Ask for help**

For You

- 1. Authenticate that it is your client (outbound calls, passphrases, etc.)**



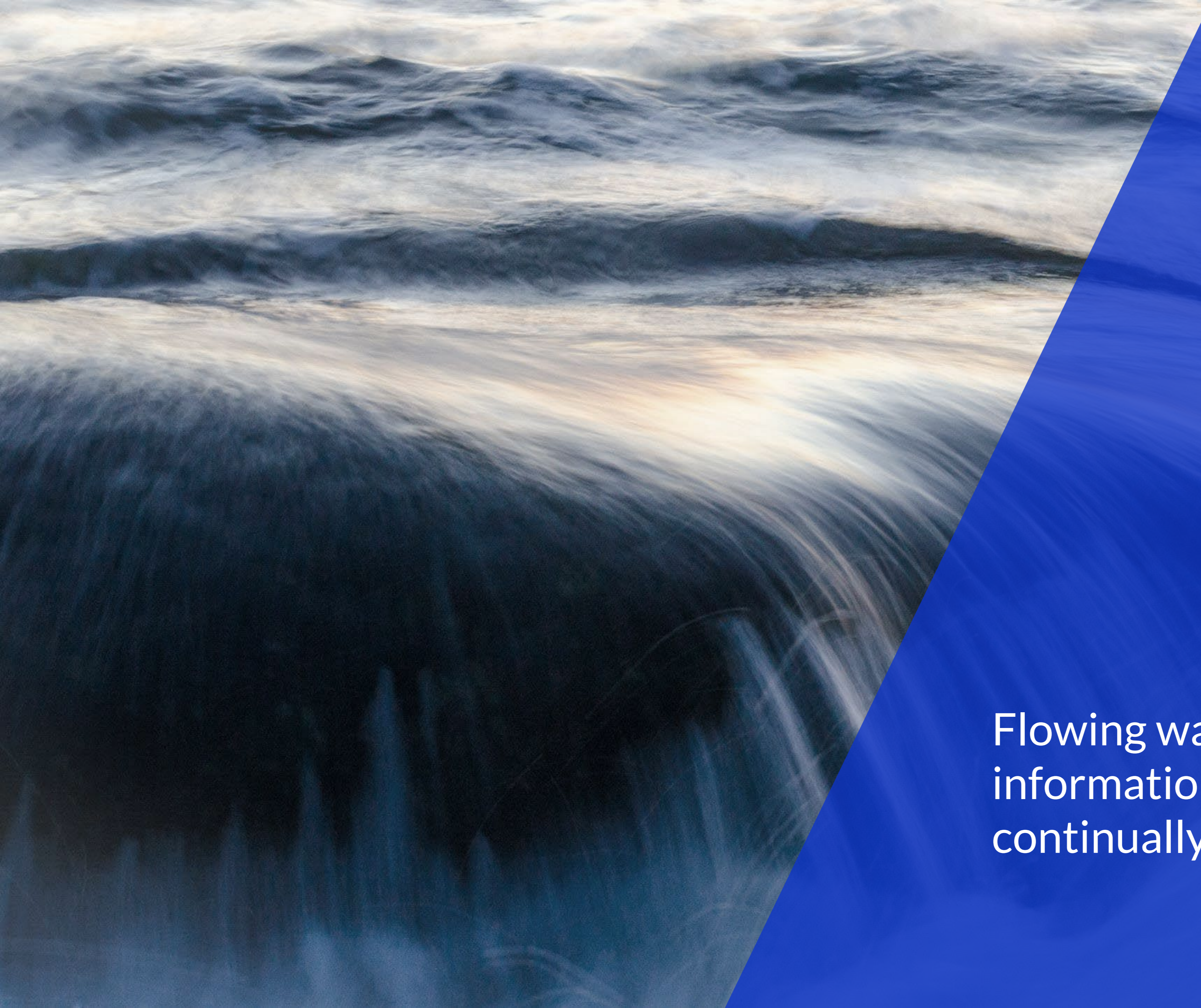
Cybersecurity for You



You might be wondering,
“What do dams have to do with
cybersecurity?”



Cybersecurity serves the same purpose as a dam – To protect and control important data by building a robust defense layer.



Flowing water is akin to the information highway. The internet is continually moving...



Dams control the water.



Cyber defenses are similar as they control and protect the flow of data.



In building a dam, one must carefully design the structure to ensure that they are able to withstand the pressure of the water else they may crack and fail.

DATA BREACH

The same holds true for protecting your organization.
If the security foundation is not properly designed and
deployed, bad things can happen.

With cyber security, one of the most important steps is to evaluate the current environment.

Organizations need to understand their current environment to deploy the appropriate protection.

Yet, several skip the planning and going straight to implementing tools which can be fatal...

Let's redefine Cybersecurity as what we will protect:



Confidentiality

Protecting information from unauthorized access and disclosure.

For example, what would happen to your company if customer information such as usernames, passwords, or credit card information was stolen?



Integrity

Protecting information from unauthorized Modification.

For example, what if your payroll information or a proposed product design was changed?



Availability

Protecting disruption in how you access your information.

For example, what if you couldn't log in to your bank account or access your customer's information, or your customers couldn't access you?

Cybersecurity is formally defined as the “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

Cybersecurity starts with a strategy

Strategic alignment

Achieving the goals and strategies through the undertaking of activities by the different governance structures or management levels .

Value delivery

Creating new value, maintaining and extending existing value, eliminating initiatives and assets that are not creating sufficient value.

Risk management

Addressing IT-related risks and using IT to assist in managing business risks.

Resource management

Having the right capability to execute the strategic plan, and providing sufficient, appropriate and effective resources.

Performance measurement

Tracking the achievement of the objectives of the enterprise and compliance with specific external requirements.

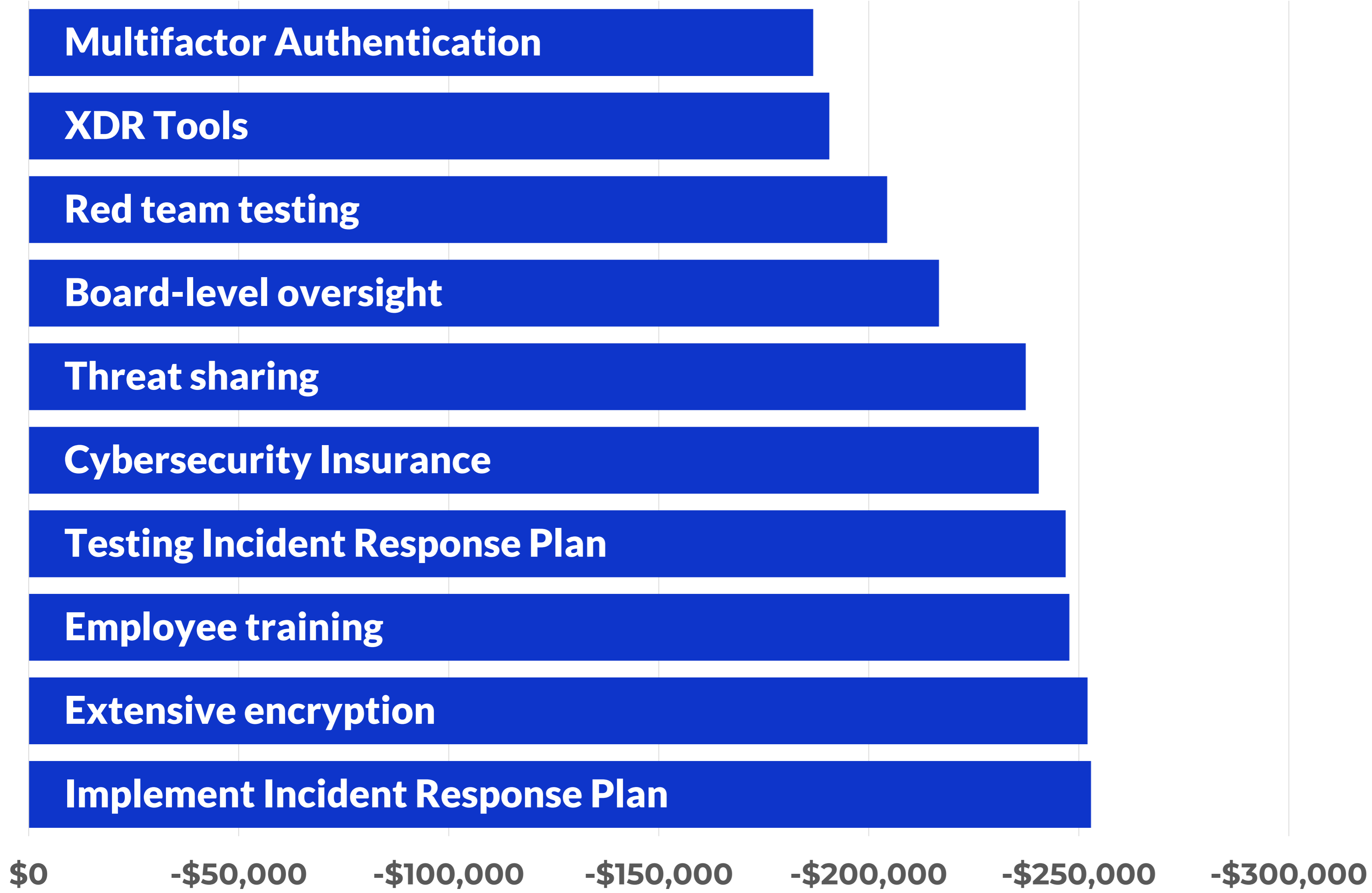


Cybersecurity Considerations

Physical Security Protection of property, e.g. using fences and locks	Personal Security E.g. using background checks	Contingency Planning How to resume normal operations after an incident
Operational Security Protecting business plans and processes	Privacy Protecting personal information	Completeness Lacking any of the aforementioned diminishes the effectiveness of others

Support and monitor People, Process, and Technology

What can you do to reduce the cost of an incident?



Average total cost of a data breach
\$4.35M

Cost of a Data Breach Report 2022

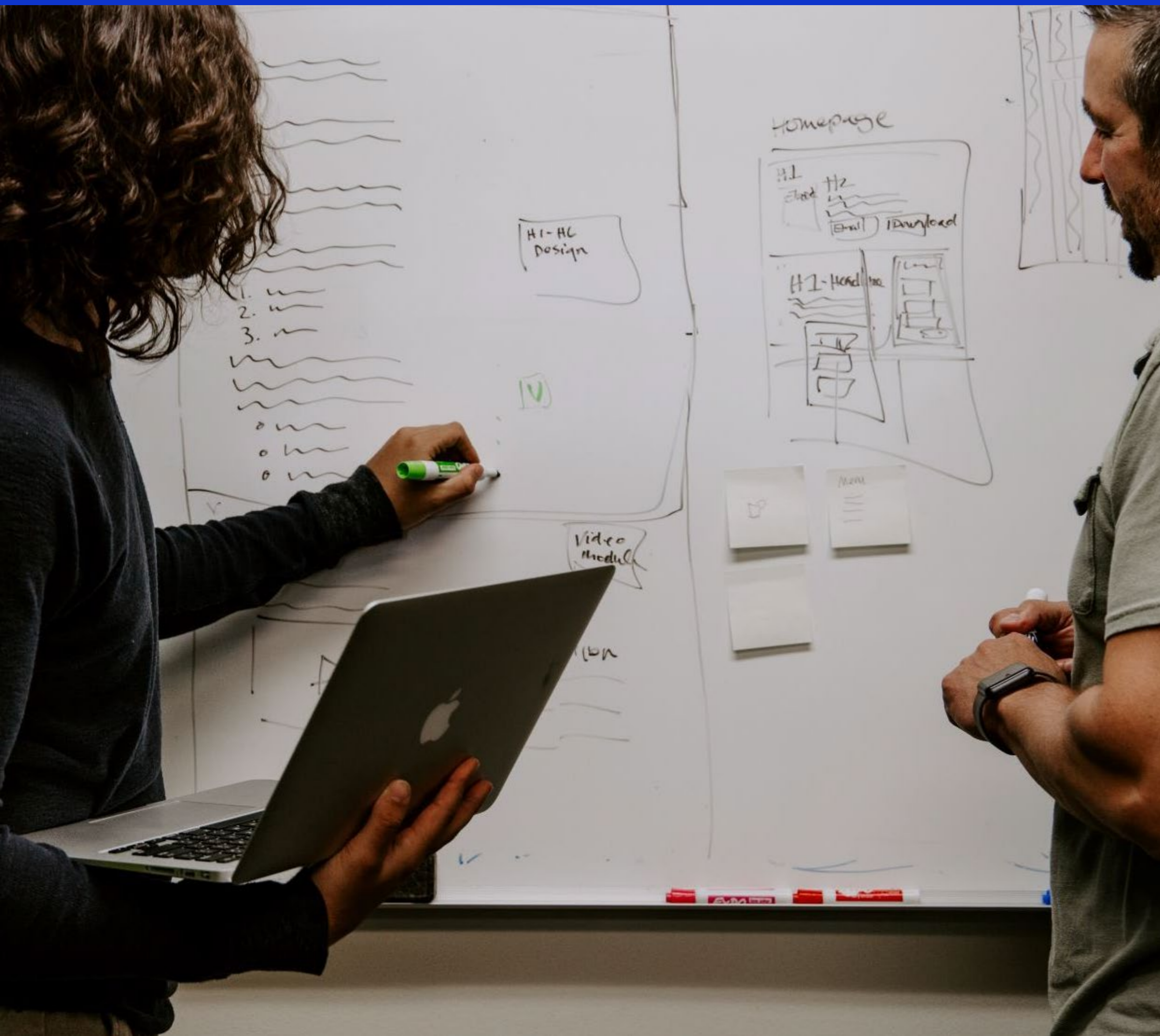
Baseline Program Protections

- Information Security Program
- Critical Asset Inventory
- Risk Assessment – Impact, Likelihood and Priority
- Back Up Strategy
- Vendor Management Process
- Incident Response Plan
- Security Control Testing





How Can We Help?



Strategy

Establish
Governance

Identify

What are the
crown jewels?

Protect

Protect the
crown jewels

Build

Deploy security
protections

Policy

Build out of
policies



Cybersecurity Standards

We routinely assist organizations with evaluating the operation of their cybersecurity controls to determine effectiveness and opportunities for improvement.

Penetration Tests

We have the “helpful hackers” who can assist organizations with determining where they are vulnerable to an attacker.

Social Engineering

Will someone physically be able to get into sensitive areas of your client’s office?

How likely are your client’s employees to click on that phishing link?

Will they answer the phone from “IT” to “fix” their computer?



Department of Defense

The DoD is expected to formally adopt a new cybersecurity standard in spring 2023.

365,000 suppliers will be required to comply to have a contract with the DoD. Suppliers are required to “waterfall” the requirement to all of their suppliers.

Financial Institutions

Since the earlier 2000s, the Gramm-Leach-Bliley Act has required that all businesses that are “significantly engaged” in providing financial products or services to consumers must have a cybersecurity program.

This includes everyone from banks to car dealerships to tax preparers.

Managed Solutions

40



Cybersecurity Training

Managing Onsite and Cloud Technology

Deploying Secure Tech Environments

Multifactor Authentication Tools

Managing Microsoft M365

Computer Security Systems



QUESTIONS