

A black and white photograph of a man with a beard, wearing a dark sweater over a collared shirt, standing in a server room. He is holding a laptop and looking down at it. The server racks are visible in the background, creating a sense of depth. A white diagonal line runs from the top right corner towards the center of the image.

# Cybersecurity and Today's Remote Workforce

**Rehmann**  
EMPOWER YOUR PURPOSE



# Presenter

2



**Paul Kennedy**

Sr Manager, IT Security Solutions | vCISO  
616.222.9200 | [paul.kennedy@rehmann.com](mailto:paul.kennedy@rehmann.com)

Paul serves as a virtual chief information security officer (vCISO) and helps lead Rehmann's IT Audit and Assessment team. In this capacity, he works with clients in the financial industry to implement, assess and improve their Technology Risk Management functions. He provides clients with peace of mind by leading cybersecurity consulting engagements, information security assessments, vulnerability and penetration testing, social engineering testing, information security training and Sarbanes-Oxley Act (SOX) 404 consulting engagements for a variety of clients.

# Our Agenda for Today

3



**Review Cyber Security Landscape**



**Proactive Security Measures**



**New Spins on Classic Security Threats**



**Action items that will empower you!**



**Cyber Risk Management**

# A New Reality

4

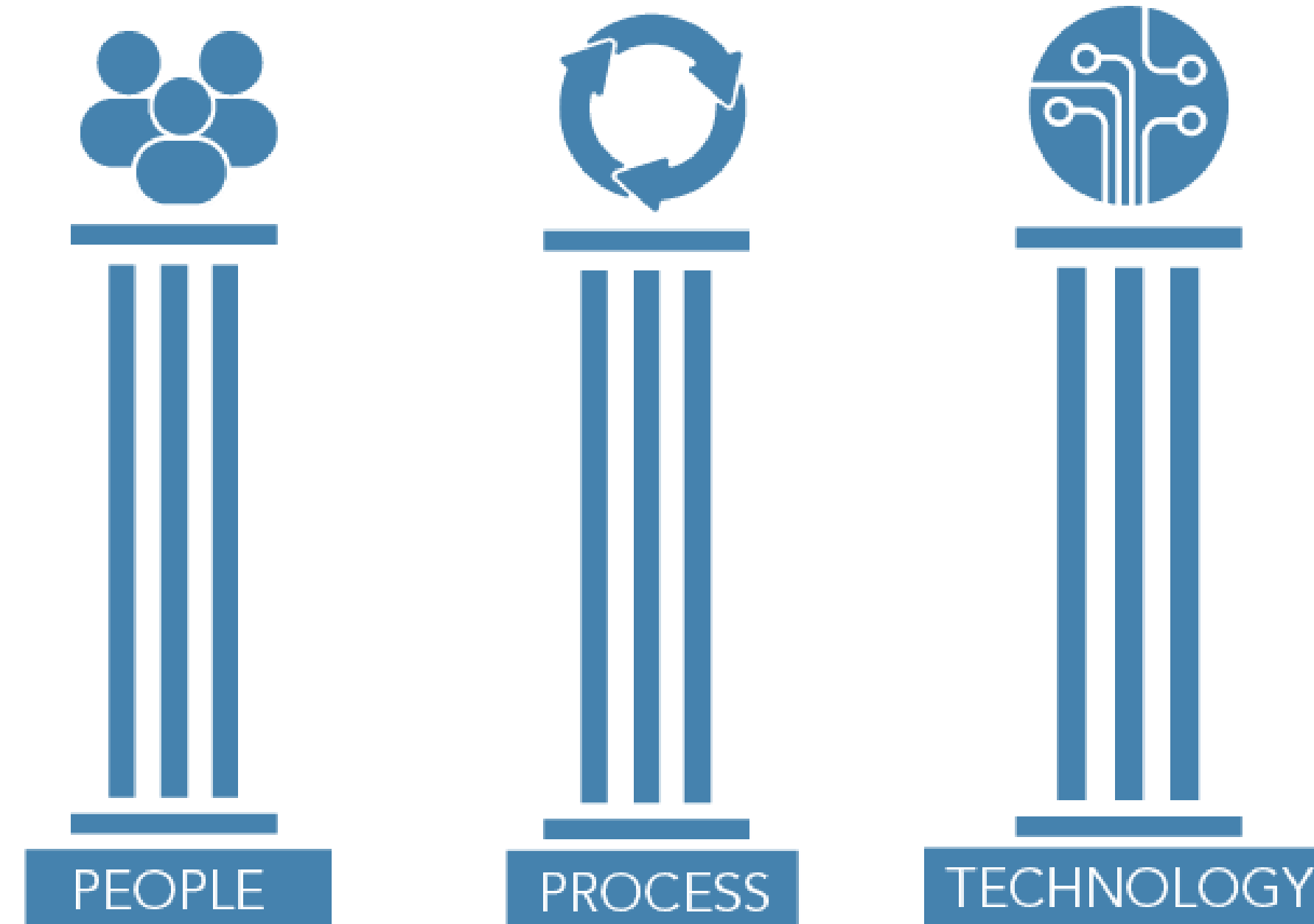
“

**There are only two types of companies:  
those that have been hacked, and those  
that will be.”**

— Robert Mueller, FBI Director, 2001-2013

# Who's Responsible for Cybersecurity?

Cybersecurity is a business issue, not just an IT issue!





# Have you seen the headlines?

6

 Infosecurity Magazine

## US Staffing Firm Hit by Ransomware Again

Commenting on the alleged second ransomware attack, Emsisoft threat analyst Brett Callow told Infosecurity Magazine: "It's not uncommon to see

...

2 days ago



## U.S. Security Agencies Issue Advisory on Russian Cyber Attacks on Infrastructure

Insurance Journal · 13 hours ago

- Mitigating Russian state-sponsored cyber threats to US critical infrastructure

Security Magazine · 9 hours ago

 [View Full Coverage](#)



 ZDNet

## Ransomware: Huge rise in attacks this year as cyber criminals hunt bigger pay days

Live. Why ransomware has become the biggest cyber threat to your network in 2020. Watch Now. There's been a huge increase in the number

...

1 week ago



 TechTarget

## Maze ransomware gang uses VMs to evade detection

A Sophos investigation into a Maze ransomware attack revealed that threat actors borrowed an attack technique pioneered by Ragnar Locker ...

1 day ago



 Threatpost

## California Elementary Kids Kicked Off Online Learning by Ransomware

The attack on the Newhall District in Valencia is part of a wave of ransomware attacks on the education sector, which shows no sign of ...

1 day ago



 FOX Carolina

## Greenville Tech confirms some info was 'accessed and ...

GREENVILLE, SC (FOX Carolina) - Greenville Technical College said Friday that the recent ransomware attack from August 27 involved a data breach.

17 hours ago



## 2021 Cyber Review: The Year Ransomware Disrupted Infrastructure

Government Technology · Dec 19   



## Opinion | The cybersecurity risk to our water supply is real. We need to prepare.

The Washington Post · 9 days ago · Opinion



## Navigating the threat of cyber attacks on the transport sector

TechRadar · 11 hours ago



# Impact cannot be ignored



Lumu  
Safety Detectives: Ransomware Facts, Trends & Statistics for 2020  
Infrascale Ransomware Survey

**\$4.24 million**

Global average cost of a data breach

**51%**

Reported a significant interruption in the last 2 years.

*“[We are] heavily reliant on the ability to deliver projects per a timeline. An attack on company software or equipment can put this in jeopardy. Few project timelines can absorb 12.1 days of reduced productivity.”*

Construction Executive Magazine

**“ Security is not convenient. ”**



# Why Do They Do It?



Then everything else...



Thrills



Idealism



State Sponsored



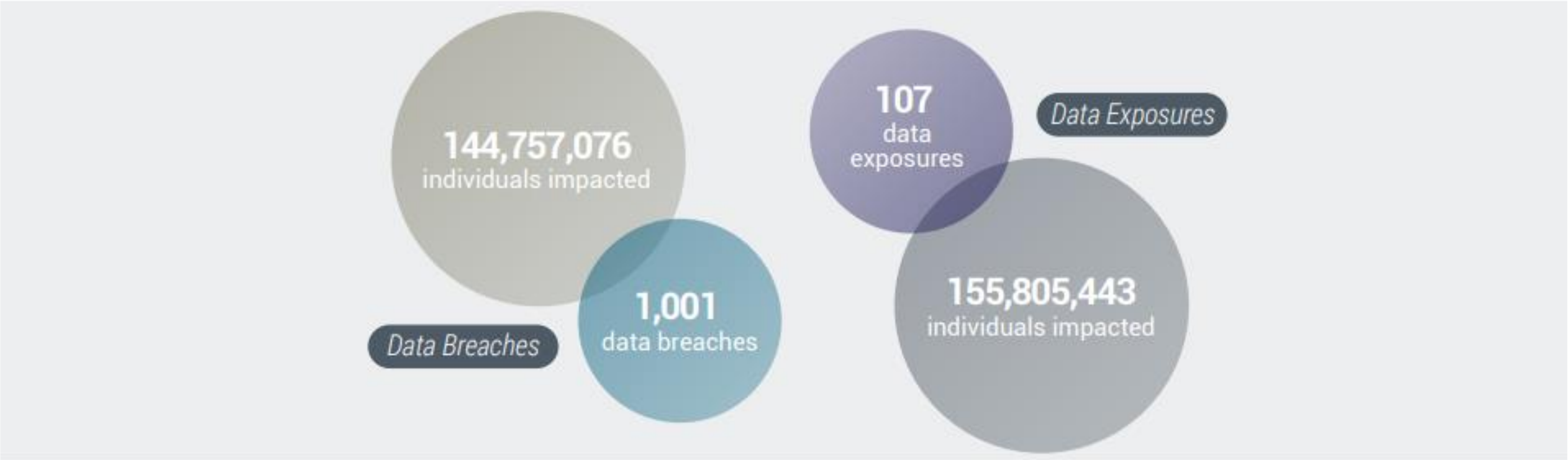
Hacktivism

# Data Breach History

## Year-Over-Year Totals\*

\* Includes third-party/supply chain compromises as single incidents, does not include individual entities affected by a third-party compromise

	2015	2016	2017	2018	2019	2020
# of Breaches & Exposures	785	1,104	1,631	1,280	1,362	1,108
# of Individuals Impacted	318,276,407	2,541,581,891	2,081,515,330	2,231,245,353	887,286,658	300,562,519

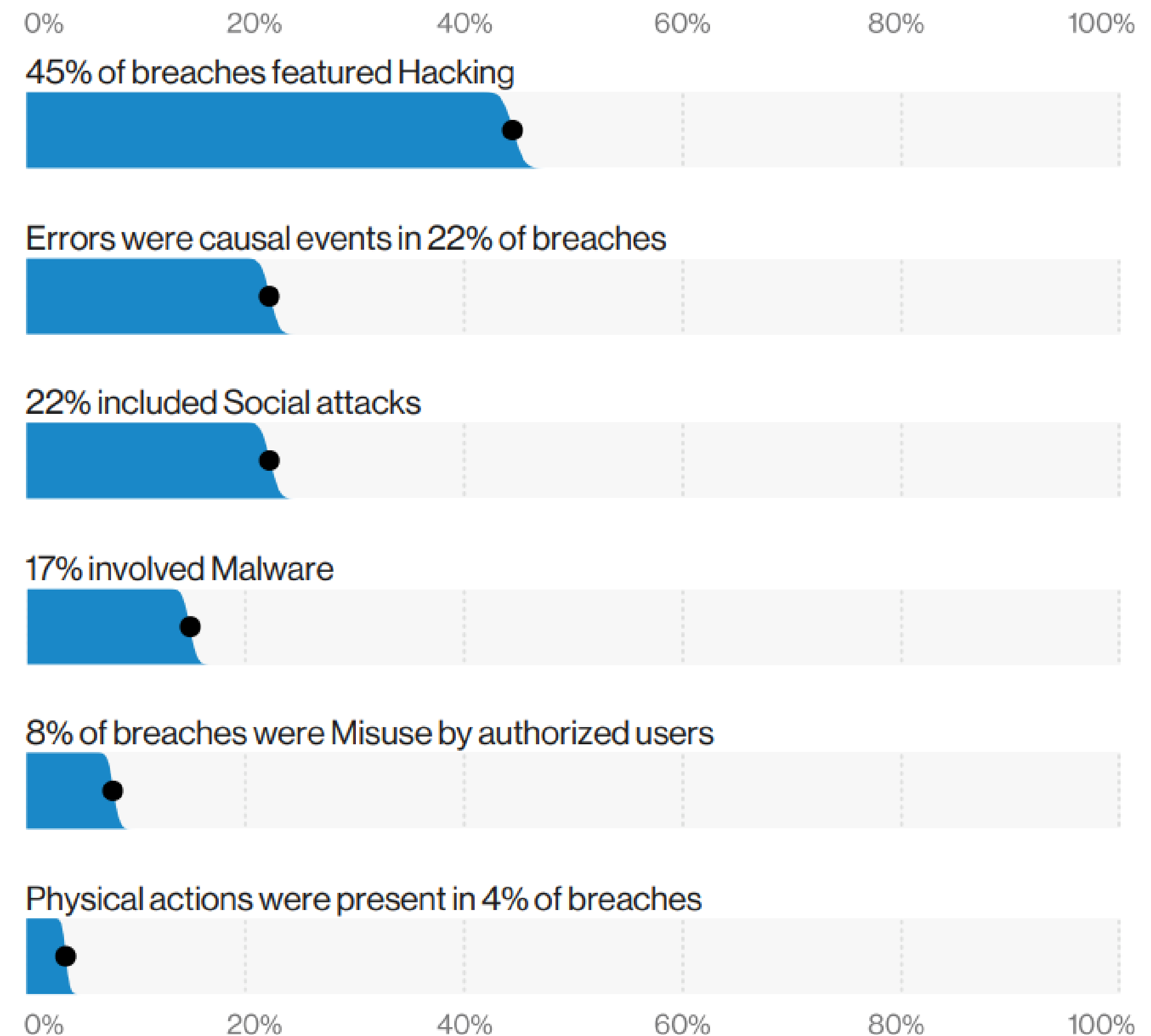


© Identity Theft Resource Center 2021 | Annual Data Breach Report | IDTheftcenter.org



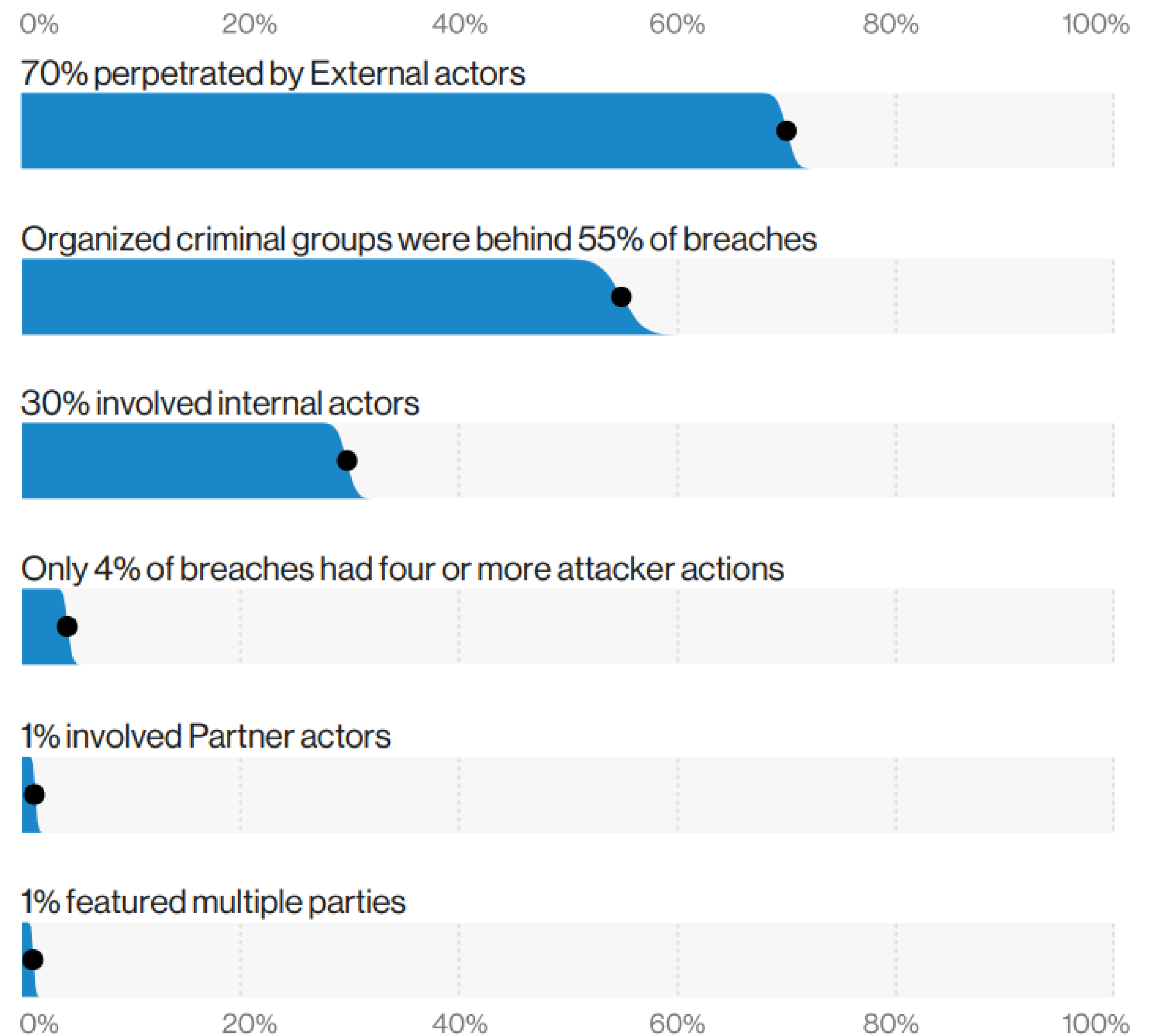
# What are the Tactics?

**Figure 2.** What tactics are utilized? (Actions)



# Who's behind the Breaches?

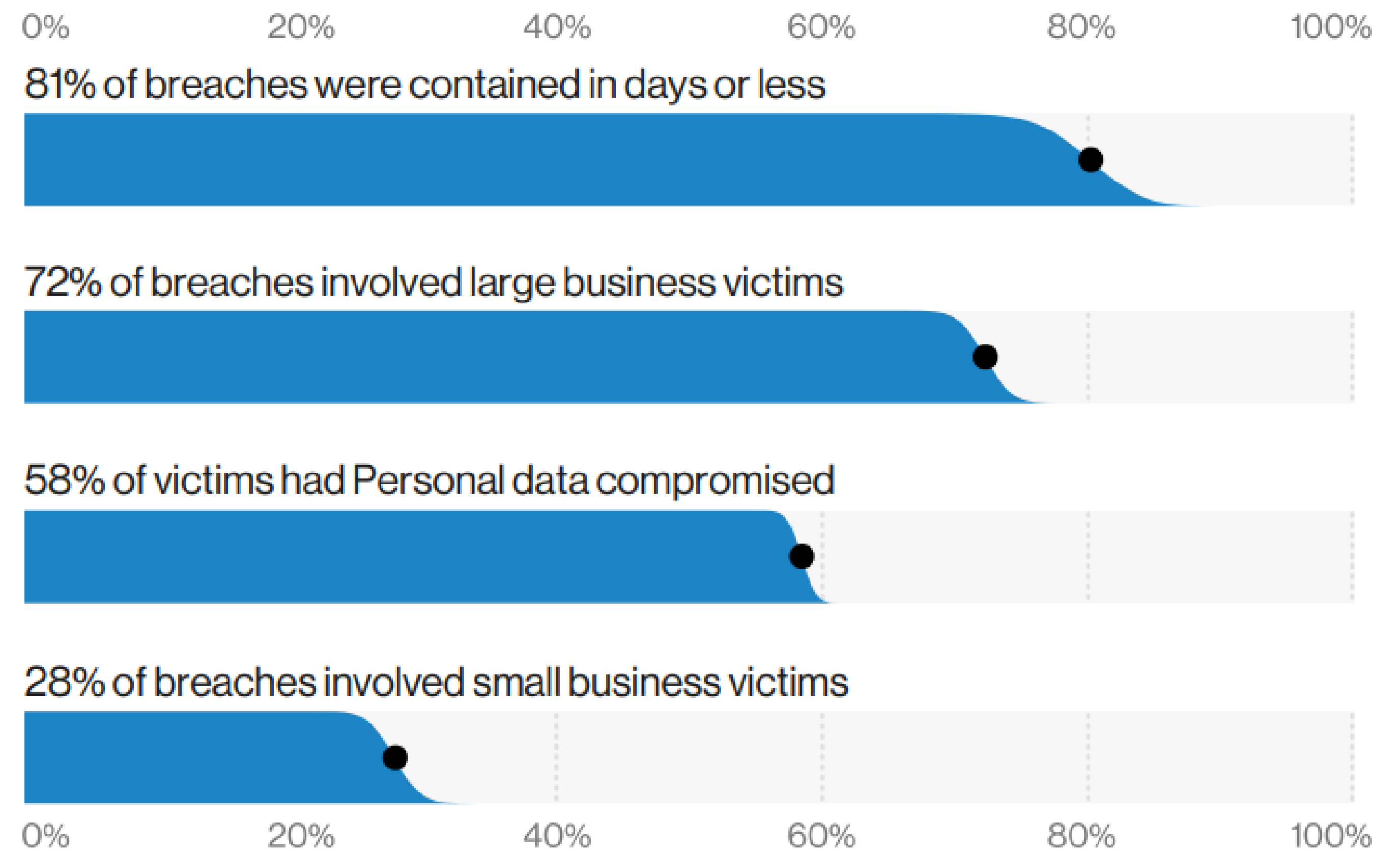
**Figure 3.** Who's behind the breaches?





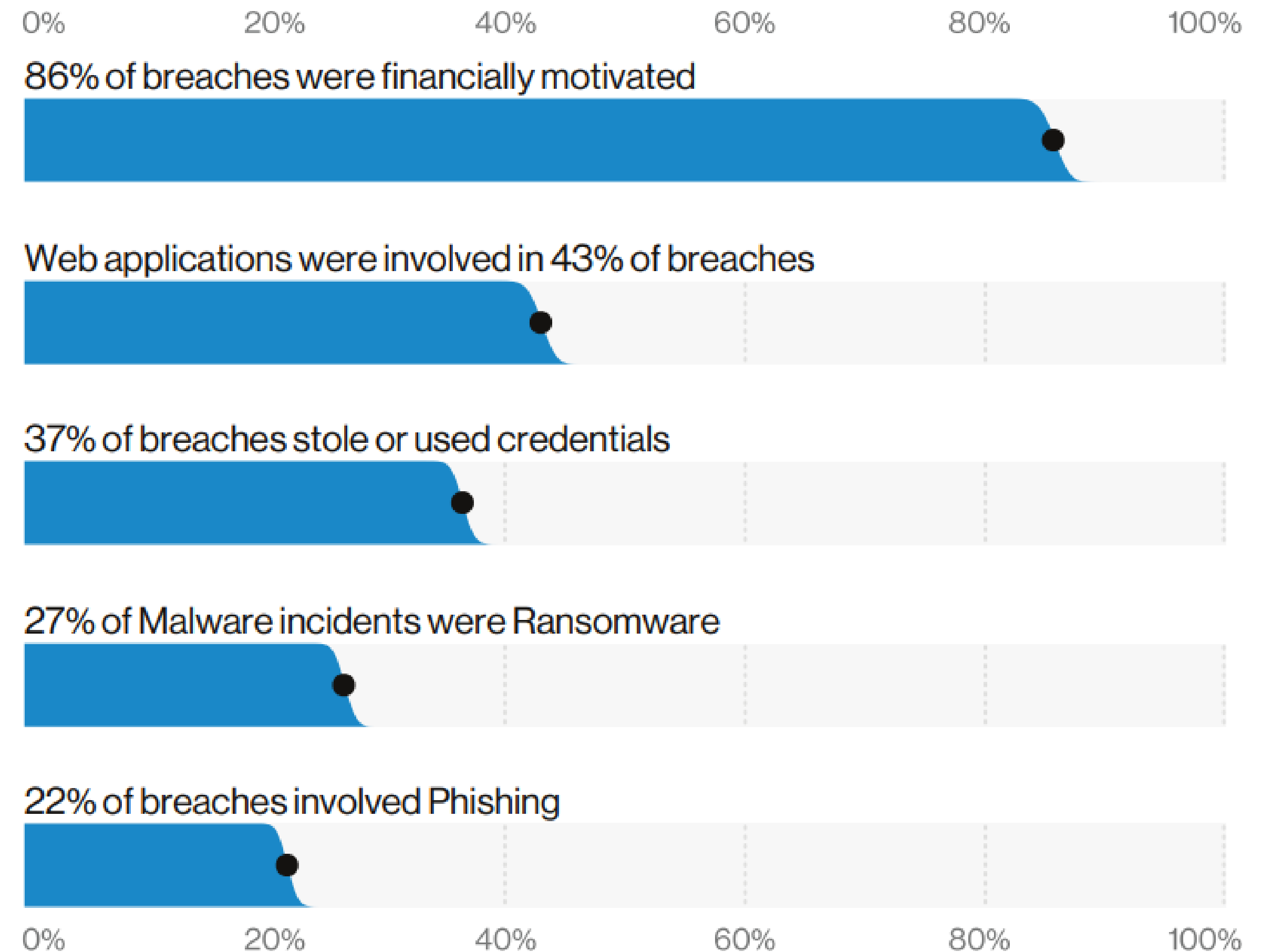
# Who are the victims?

**Figure 4.** Who are the victims?



# What do they have in common?

**Figure 5.** What are the other commonalities?





A person wearing a dark hoodie is sitting at a desk, working on a laptop. The person's face is obscured by the hood. The background is dark with some white geometric lines. A blue semi-transparent banner is at the bottom of the image, containing white text.

# **Breach Cost: What is Your Exposure?**



# Ponemon 2021 - Cost of Breach

16

## 10%

Increase in average total cost of a breach, 2020-2021

---

The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years.

---

The average per record (per capita) cost of a data breach increased 10.3% from 2020 to 2021.

In 2021 the per record cost of a breach was \$161, compared to an average cost of \$146 in 2020. This represents an increase of 14.2% since 2017 report, when the average per record cost was \$141.

## 287

Average number of days to identify and contain a data breach

---

The longer it took to identify and contain, the more costly the breach.

---

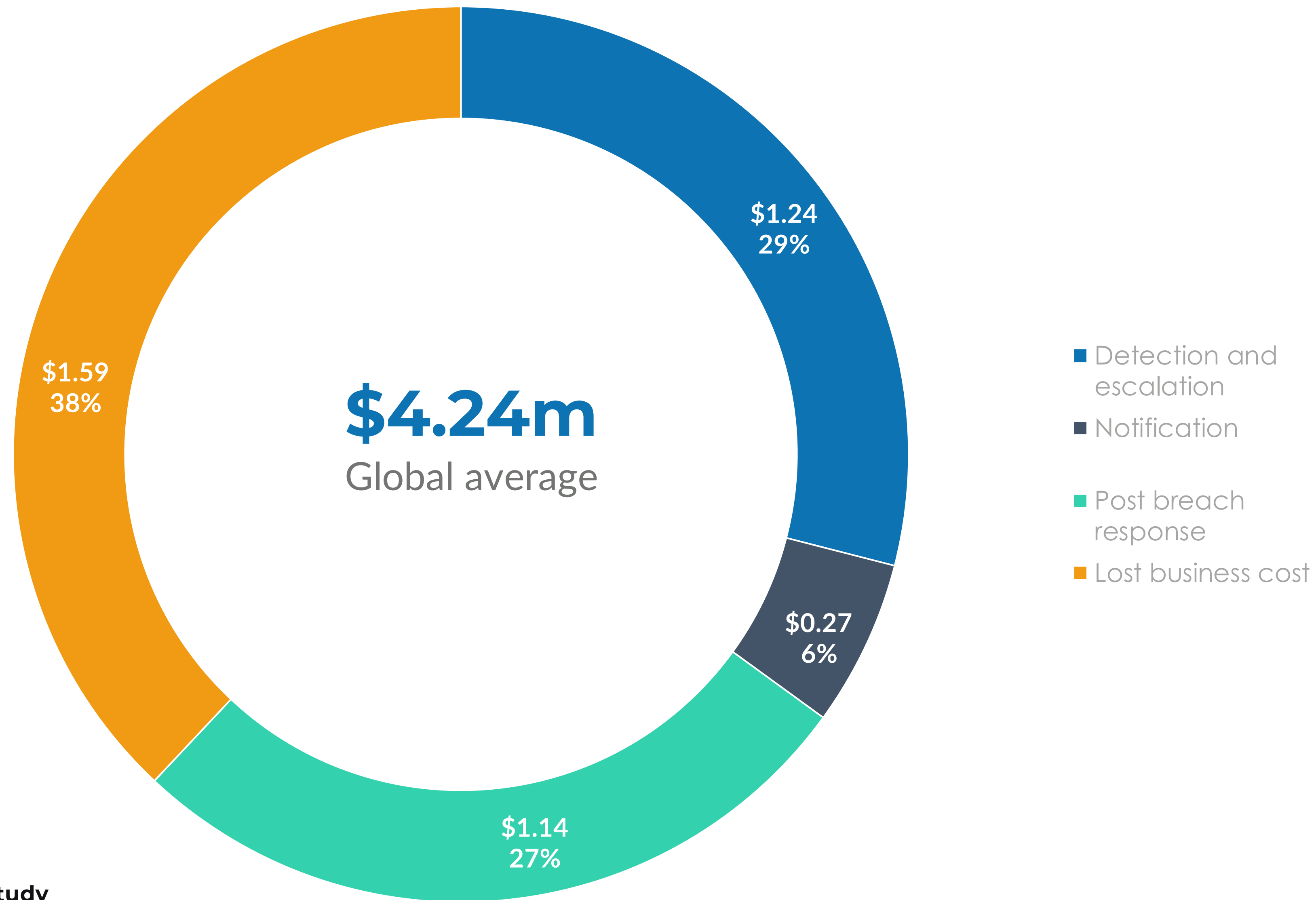
## 51%

Amount of organizations reporting a **significant business disruption** during the past two years due to a cybersecurity incident.



# Ponemon 2021 – Data Breach Root Causes

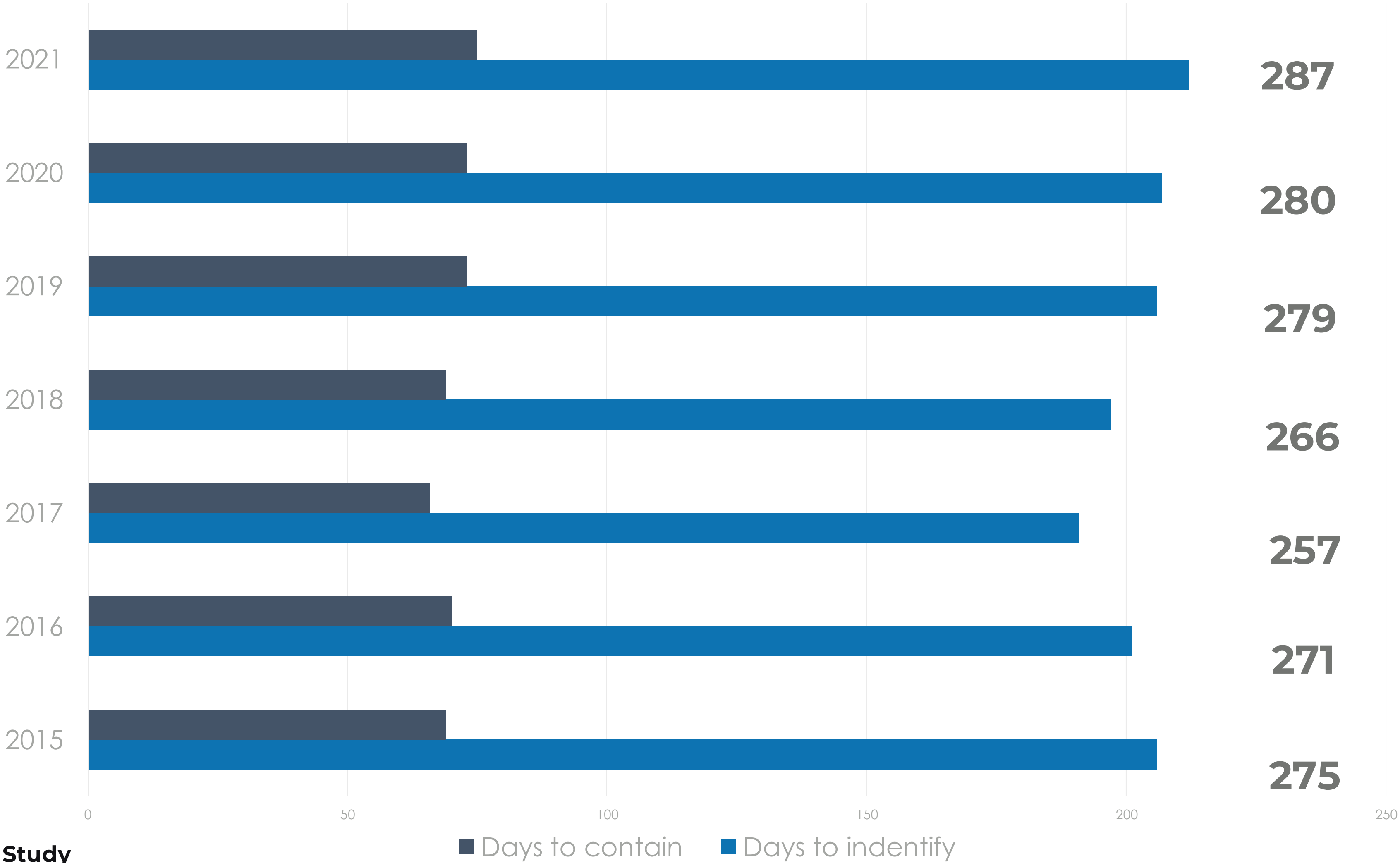
17



Reference: Ponemon Study

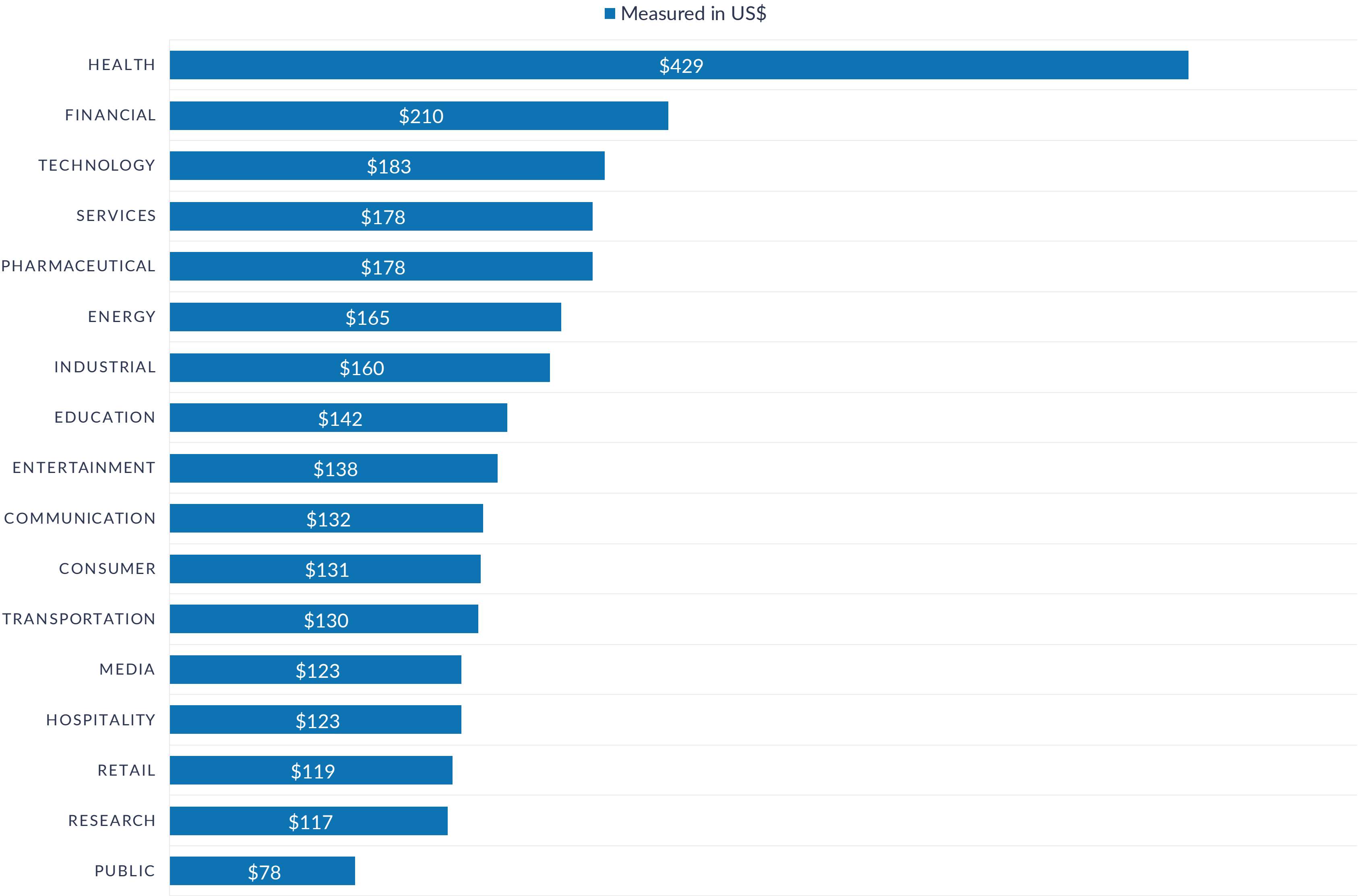
# Ponemon 2021 – Key Facts

Average time to identify and contain a data breach  
Measure in days



Reference: Ponemon Study

# Average Cost Per Record by Industry Sector



Reference: Ponemon Study



# Potential Exposure SWAG Calculation



## Records-based cost










Number of Records with PII  $\times$  \$161 per record  $=$  Exposure

## Average downtime cost

Downtime cost per hour  $\times$  Average time to recover  $=$  Exposure

Personally Identifiable Information (PII)

# Threat Vectors – How the Bad Guys Get In

 Phishing, Web & Ransomware	 Compromised Credentials	 Weak Passwords
 Trust Relationships & Propagation	 Poor Encryption	 Unpatched Vulnerabilities
 Misconfigurations	 Malicious Insiders	 Zero Day & Unknown Methods



# COVID Phishing Emails

*"Distributed via the CDC Health Alert Network  
January 31, 2020  
CDCHAN-00426*

*Dear [REDACTED]*

*The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.*

*Updated list of new cases around your city are available at ( <https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html> )*

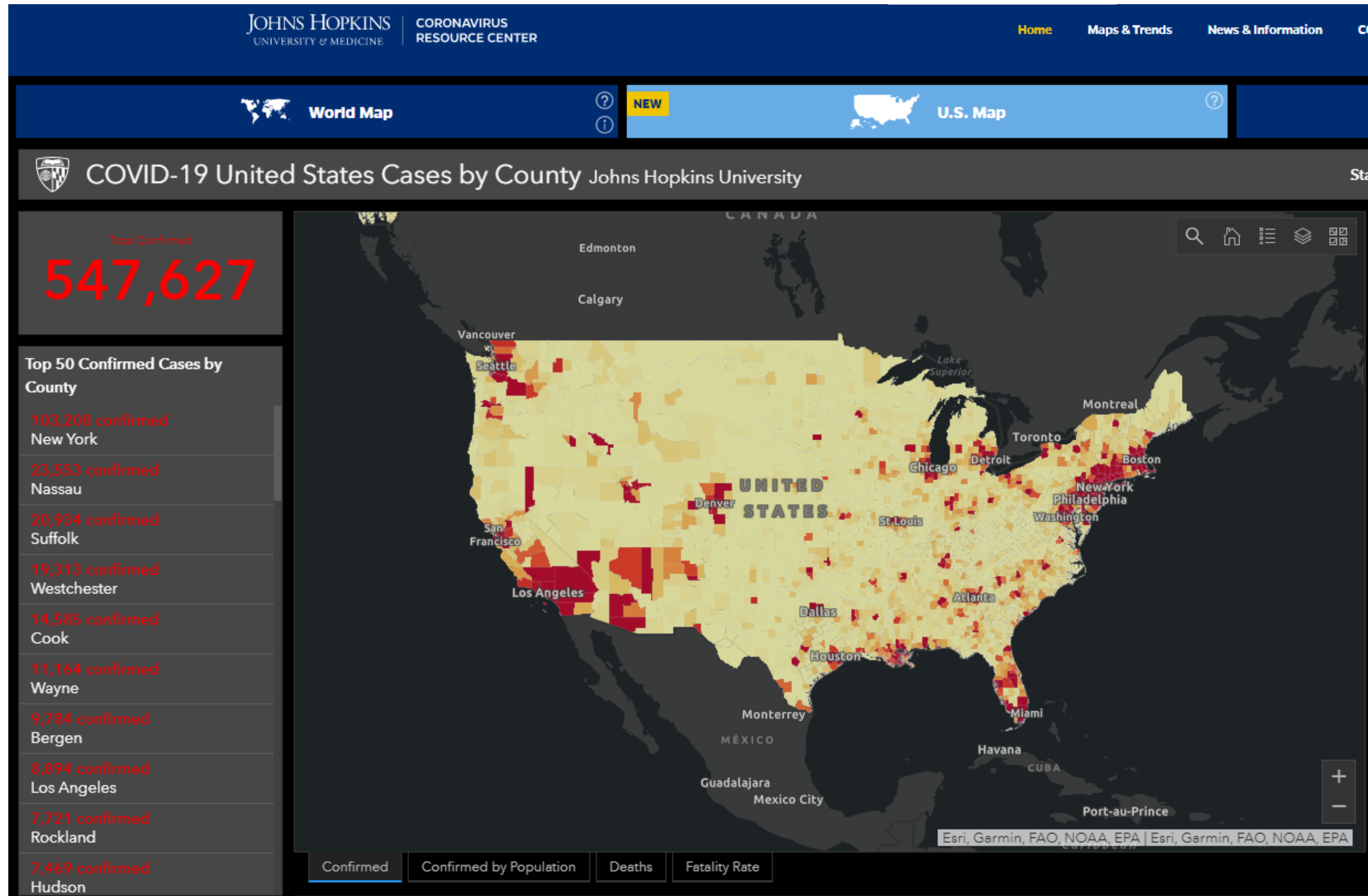
*You are immediately advised to go through the cases above for safety hazard*

*Sincerely,  
CDC-INFO National Contact Center  
National Center for Health Marketing  
Division of eHealth Marketing  
Centers for Disease control and Prevention"*



# COVID Malicious Sites

23



## Infection kits

- \$200-\$700
- Displays same map
- Deploy malware

Legitimate site:

<https://coronavirus.jhu.edu/us-map>

## Ransomware-as-a-Service

- \$500-\$2000
- Minimal hacking experience required
- Full Help Desk Support
- Easy to get in-the-game





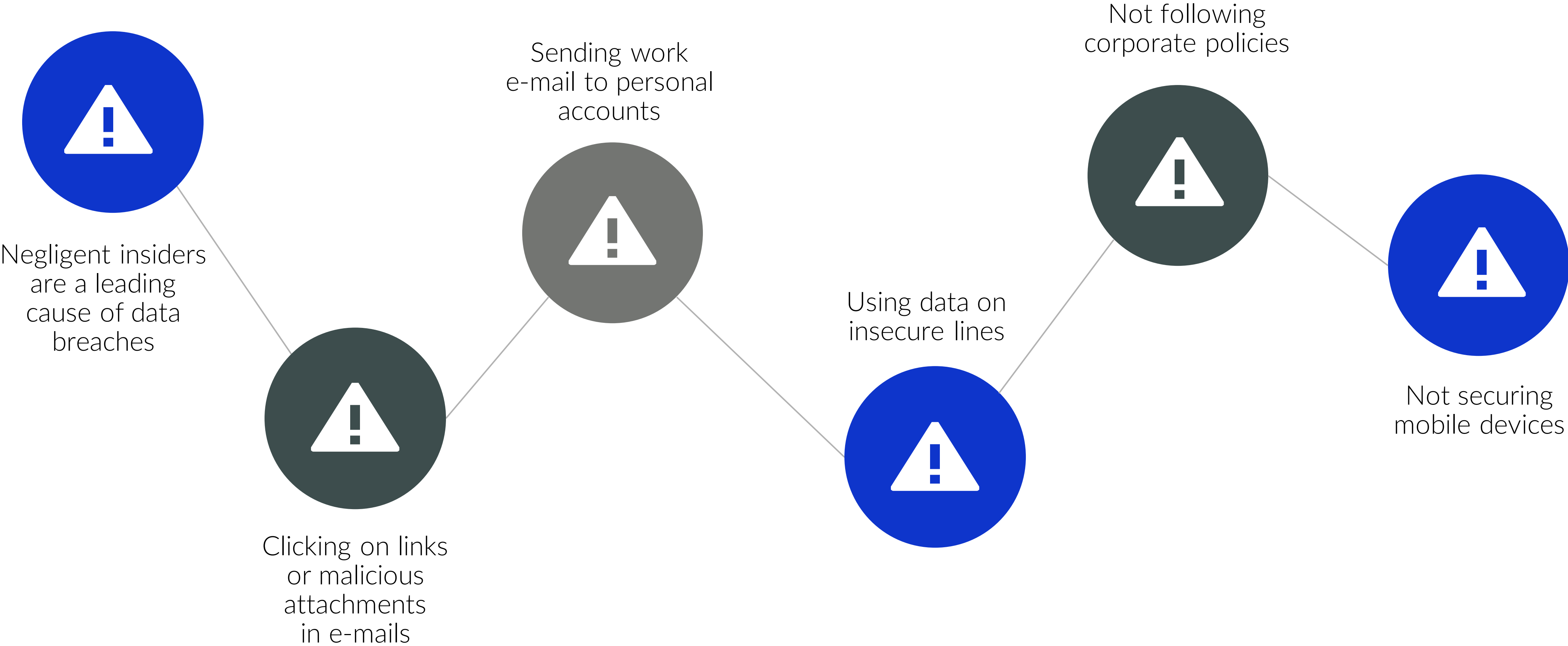
## Deepfakes will be the next frontier for enterprise fraud

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.



# Employees are the Weakest Link





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	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

**TIME IT TAKES  
A HACKER TO  
BRUTE FORCE  
YOUR  
PASSWORD**



-Data sourced from [HowSecureismyPassword.net](https://howsecureismypassword.net)



# The four cost centers of a breach



## Detection and escalation

Activities that enable a company to reasonably detect the breach.

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards



## Notification

Activities that enable the company to notify data subjects, data protection regulators and other third parties.

- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts



## Lost business

Activities that attempt to minimize the loss of customers, business disruption and revenue losses.

- Business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill



## Ex-post response

Activities to help victims of a breach communicate with the company and redress activities to victims and regulators.

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines



# Difference from average total cost of US \$3.86 million

## How Factors Increased or Decreased the Total Cost of a Data Breach



Source: IBM Security – Cost of a Data Breach Report 2020



# Incident Response

---

## 2020 Incident Response Services

(13) Ransomware Recoveries

- Non-Managed Average Spend (Labor)
  - \$70,000
- Managed Average Spend (Labor)
  - \$15,772
- Combined Recovery Labor Spend (All)
  - \$557,481

## Matter of Compromise

- VMWare Virtual Machine Encryption
- Legacy 2003 / 2008 Windows Server
- Clicked links & attachments-Emotet & TrickBot
- Remote Worker VPN (Out-of-date Software)
- Brute Force Remote Desktop Login Password
- Citrix Compromise
- Business Email Compromise (MITM)

## Observations

- Double Extortion
- No / Limited Cyber Liability Insurance
- Backup Systems Compromised
- Limited Depth of Logging
- No Security Awareness Training
- Lack of Layered Defense
- Weak Password Policies
- Legacy Systems & Technology Debt
- Patching & Firmware Out-of-Date
- No Incident Response Planning
  - Incident Response Plan
  - Business Continuity
  - Disaster Recovery

# What do we do now???

30





# Where Should You Focus?

31

- Data
- Perimeter
- Access
- Governance
- Vendor
- Mobile
- Human





# Data Management

# Data – What is it and where is it exactly?

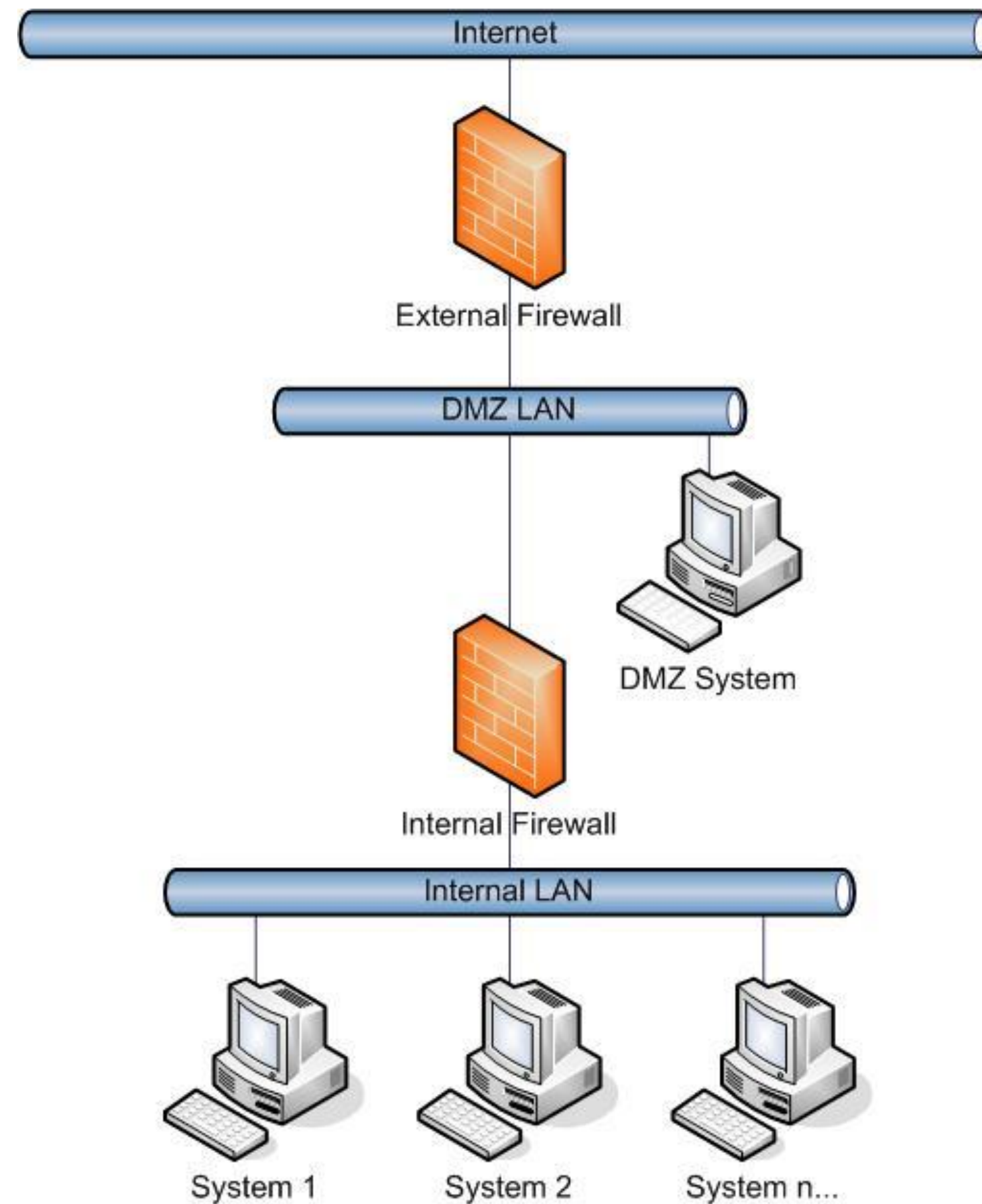
- File servers, databases, e-mail servers
- Who should have access?
- How many copies exist and where are they located?

## Risks – What is it worth?

- Does it contain PII?
- Does it contain sensitive information?



# Perimeter Management



Do you have an external DMZ?

- E-mail server
- Web server
- FTP server

Do you have or need an internal DMZ to maintain confidentiality?

- SQL server
- File shares



# Access Management

- Access Control
- Restrict Administrative Access
  - Users
  - Service Accounts
- Perform Access Reviews
  - Full access reviews at least annually – include service accounts
  - Admin reviews monthly/quarterly
- Leverage Least Privilege
- Multi Factor Authentication





# Governance



# Vendor Management

- Selection Due Diligence
- Contract Reviews
- Annual Due Diligence





# Mobile Device Management

- Acceptable Use Agreements
- Authentication & Encryption
- Secure Transmission
- Device Management
- Employee Training



# Training for Employees

- Perform on a regular basis
- Educate about threats & best practices
- Phish your employees and use the results for education







# Top Recommendations

---

1. Establish Cyber Risk Ownership & Oversight
2. Establish Policies & Procedures (Acceptable Use, HR and Governance Policies)
3. Multi-Factor Authentication (VPN, O365, LOB, Cloud Apps)
4. Verify Backup Position & Ensure Recoverability (Offsite, Tested, Air-Gapped)
5. Incident Response & Disaster Recovery & Business Continuity Plan
6. Endpoint Detection & Response
7. Endpoint Web Content & DNS Filtering
8. Vulnerability Assessment & Pen Test (Identify Risk)
9. Cyber Liability & Crime Insurance
10. Security Awareness Training
11. All remote connections are VPN with MFA (Limit VPN Access)
12. Vendor & Patch Management
13. Password Management

## Bonus:

- Remove Admin Rights from User Workstations
- Separate Administrator accounts from base user accounts





QUESTIONS





THANK  
YOU

Rehmann is a financial services and business advisory firm. We are better at helping clients because we take a collaborative, personalized approach and build a customized team of specialists to help them achieve their objectives. We focus on the business of business – allowing people to focus on what makes them extraordinary.

The firm started as a CPA firm 80 years ago. Now, we are a multifaceted advisory firm that helps businesses and high-net-worth families maximize potential. Clients who work with us want us to be more than a vendor. They want collaboration, innovation and continuous improvement.

**Rehmann**