Cybersecurity Survival in 2020 and Beyond

Looking Inside Your Virtual Walls

October 27, 2020

Segal

Today's Presenters and Their Perspectives

Christopher Nickson
Senior Consultant

Employer Confidentiality

Jay Preall
Senior Consultant

Insider Cyber Risks and Threats

Mark Dobrow
Vice President, Consultant

Ways that Insurance Can Help Mitigate Risks

Employer Confidentiality

Traditional Employer Confidentiality Issues

Employee Medical and Health Records

Record Types: Application/enrollment forms for health insurance benefits, drug testing results, workplace injury and related OSHA records, workers' compensation records, FMLA and paid leave records

Statutes Implicated: GINA, OSHA, FMLA, HIPAA

Threat: Co-employee or manager/ supervisor gaining physical access to medical and health records

Why: Manager making discriminatory employment decision (hiring, termination, promotion) based on medical and health status or genetic information; unauthorized disclosure of medical and health records

Action: Maintain employment/personnel file for employee physically separate from employee medical and health records; limit access to records to necessary managers/supervisors

Traditional Employer Confidentiality Issues

Employee Disability and Accommodation Documentation

Record Types: Medical records or reports from employee's physician or independent medical examination provider documenting return-to-work and/or disability status and associated limitations

Statutes Implicated: Americans with Disabilities Act (ADA) and various state anti-discrimination laws

Threat: Co-employee or manager gaining unauthorized physical access to disability and accommodation records

Why: Manager making discriminatory employment decision (termination, promotion) based on disability status

Action: Limit access to medical records and reports

Traditional Employer Confidentiality Issues

Other Types of Employee Records

Record Types: Documents supporting I-9s (driver's license, Social Security number, passport, immigration records), workplace investigations, performance reviews, disciplinary records, background checks, payroll records

Statutes Implicated: Privacy laws

Threat: Co-employees or third-parties gaining access to on-site stored records

Why: Manager making discriminatory employment decision (termination, promotion) based on immigration status

Action: Locked file cabinets or record rooms; segregation of records; use of unique employee identification numbers unrelated to SSN

Cybersecurity Employer Confidentiality Issues

Employee Records

Record Types: Employee medical and health records, employee accommodation documentation, and other employee records

Statutes Implicated: GINA, OSHA, ADA, HIPAA, privacy laws

Threat: Employee or third-party gaining unauthorized access remotely through intrusion; employees gaining access to co-employee records via shared drive or common point of access

Why: Third-parties selling information or holding information for ransom

Action: Take cybersecurity precautions like:

- Encrypt data and records
- Perform regular phishing tests of your staff
- Purchase cyber liability insurance

Insider Cyber Risks and Threats

Quick Quiz About Cybersecurity

Question 1 (of 4)

Which of these receives the most hits on Google?

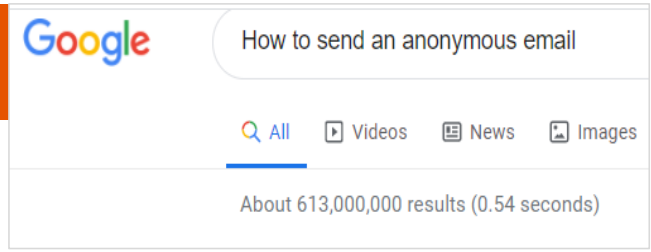
- Best Mother's Days gifts?
- How to hit a baseball?
- How to make a cherry pie?
- How to send an anonymous email?

Answer:

Sending a fake email receives **more than three quarters of a billion hits!!**

Best Mother's Days gifts?	99M
How to hit a baseball?	327M
How to make a cherry pie?	96M
How to send an anonymous email?	**613M**

Mom, baseball, and cherry pie added together do not beat how to send an anonymous email!



Google searches performed on October 14, 2020

Question 2 (of 4)

According to the 2017-2019 Verizon Data Breach Investigations reports, of all the cybersecurity attacks that occurred, what percentage of those attacks were related to internal actors in 2018?

- ○ 40%
- ○ 34%
- ○ 28%
- ○ 22%
- ○ 16%

Internal actors are defined as:

- Careless workers who ignore cybersecurity policies because it is faster for them to get their work done
- Inside agents recruited by third parties to steal or corrupt data
- Disgruntled workers seeking revenge
- Employees actively seeking to profit from stolen information
- Third party users, who are vendors, with all of the same above problems.

Answer:

Your own employees represent one third of the risk for a cybersecurity incident occurring!

40%

34%

28%

22%

16%

The majority of issues with ‘internal actors’ occur because employees simply make mistakes, such as clicking on a phishing email, and the organization does not have the tools, training, and processes in place to prevent those mistakes from causing major damage.

Google searches performed on October 14, 2020

Question 3 (of 4)

What was the average cost of an insider incident for an organization in 2020 in these three categories: employee or contractor negligence / criminal/malicious insider / credential thief?

- ○ $307K $756K $872K
- ○ $291K $665K $813K
- ○ $278K $604K $672K
- ○ $255K $494K $579K
- ○ $207K $347K $493K

Source: 2020 Global Cost of Insider Threats Ponemon Report

Answer:

Approximately one third of these costs are direct costs while the remaining costs are indirect, such as impact on productivity, reputational damage, etc.

employee or contractor negligence	criminal/ malicious insider	credential thief	
$307K	$756K	$872K	
$291K	$665K	$813K	
$278K	$604K	$672K	This was the cost in the year 2018
$255K	$494K	$579K	
$207K	$347K	$493K	This was the cost in the year 2016

The activities that drive costs are: monitoring & surveillance, investigation, escalation, incident response, containment, ex-post analysis and remediation. Expect to pay an average of $103K just for the investigation of what happened!

Source: 2020 Global Cost of Insider Threats Ponemon Report

Question 4 (of 4)

What was the average time required to contain an insider incident for an organization in 2020?

- ○ 13 days
- ○ 39 days
- ○ 55 days
- ○ 77 days
- ○ 104 days

Source: 2020 Global Cost of Insider Threats Ponemon Report

Answer:

77 days is a lot of time for dedicating your staff to containing an insider incident. On average, only 13% of incidents were contained in less than 30 days.

13 days

39 days

55 days

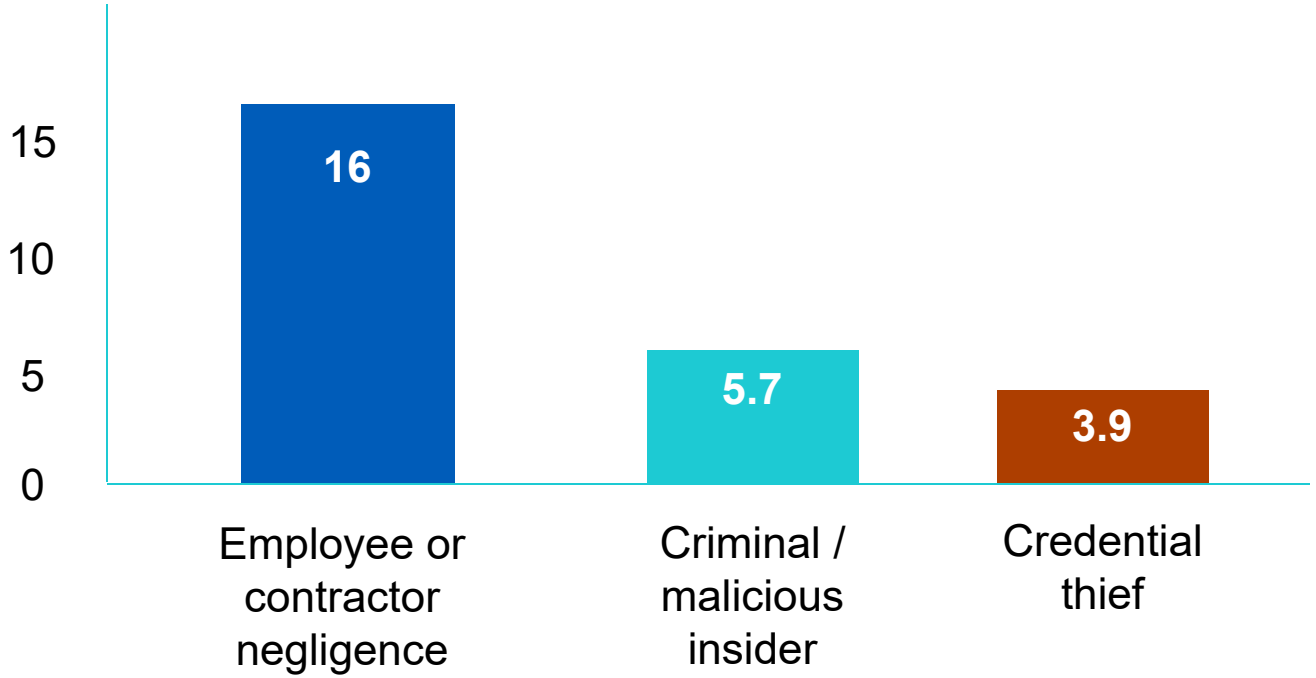
77 days

104 days

Source: 2020 Global Cost of Insider Threats Ponemon Report

Average Annual Insider Incident Frequency

(for 204 surveyed U.S. organizations in 2020)



Source: 2020 Global Cost of Insider Threats Ponemon Report

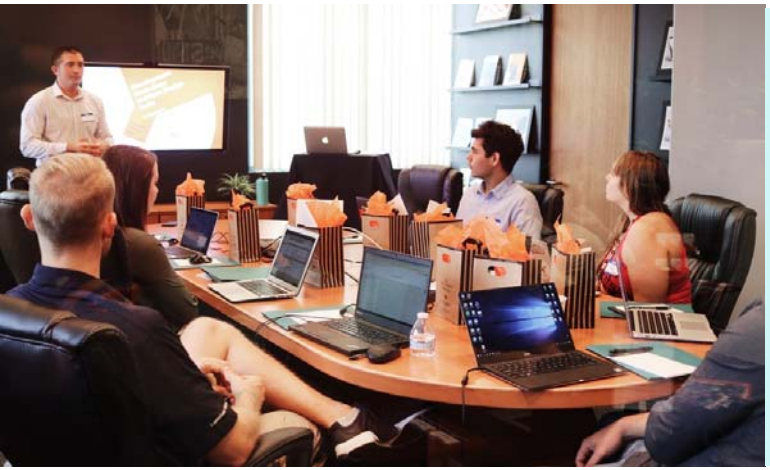
Who are the Insiders?

Employees

Contractors

Trusted business associates

Insiders know where your confidential data is located, who has access to it, and what protections are in place (or not) to secure it.



The insider doesn't have to be a current member of your organization. They can be a former employee who still has access to proprietary or sensitive information.

What are the Insider Threats?

Careless users – neglect or bypass the security rules

Malicious insiders – use their legitimate data access for personal gain

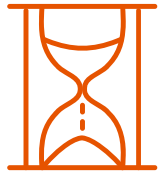
Inside agents – recruited by external parties to steal, sabotage, or delete confidential data

Activist insiders – seek to punish organizations for their stance, or lack thereof, on hot button issues

Vengeful insiders – punish organizations for some perceived personal slight

3rd parties – have access to your data and all the same reasons as above to be a threat

Table Top Exercise – Digital Blackmail



The Scenario

You have just received an anonymous email from someone claiming to have stolen 4,110 participant health records from your organization. They have included 5 sample records to prove they have real data and are demanding $40,000 in bitcoins to stop them from releasing all of the information to the public media two days from now.

What do you do next and what information should you know to respond appropriately?

- ✓ Determine if the sample data is real and from your systems.
- ✓ Identify where the sample data came from.
- ✓ Involve your cyber insurance company and/or law enforcement.
- ✓ Identify how the blackmailer accessed the data.
- ✓ Prevent further access to the data.
- ✓ Establish communications with the blackmailer.
- ✓ Decide if you are going to pay the blackmail demand.
- ✓ Save evidence for later prosecution if the blackmailer turns out to be an insider or a criminal who gets caught.

Preventing Insider Threats

What can you do to protect your organization?

Classify Your Data

Classify around these concerns…

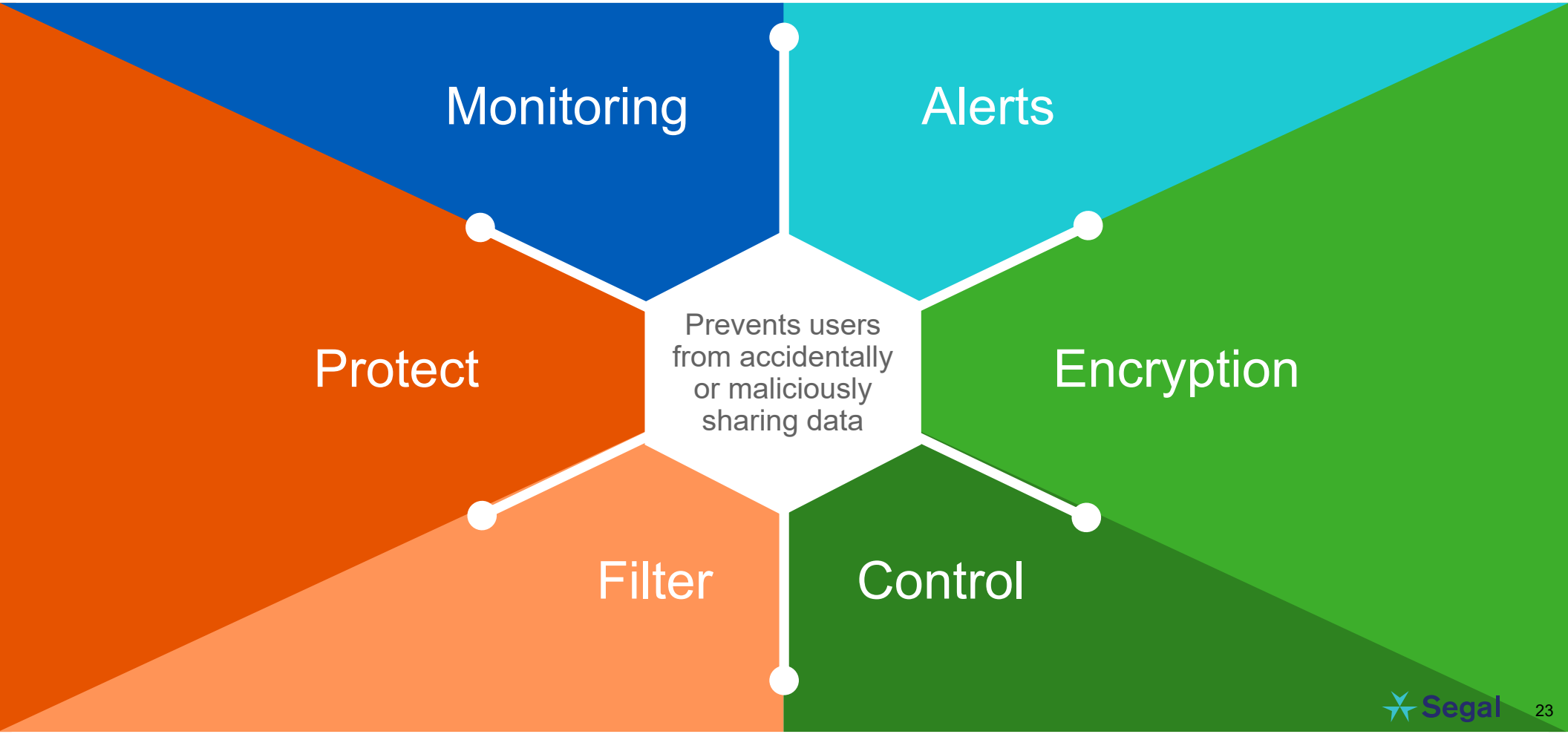
and be able to answer these questions

Who has accessed your data?

When did they access it?

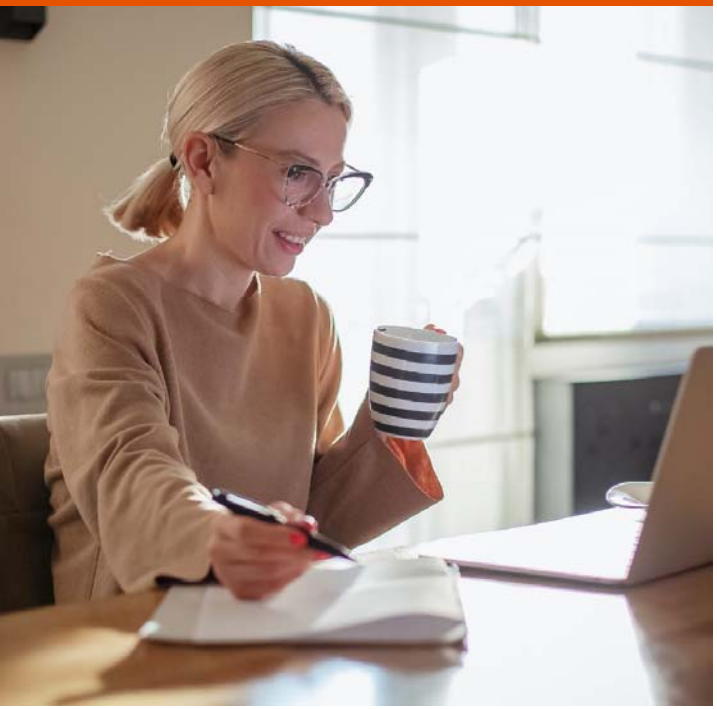
What data did they access?

Data Loss Prevention

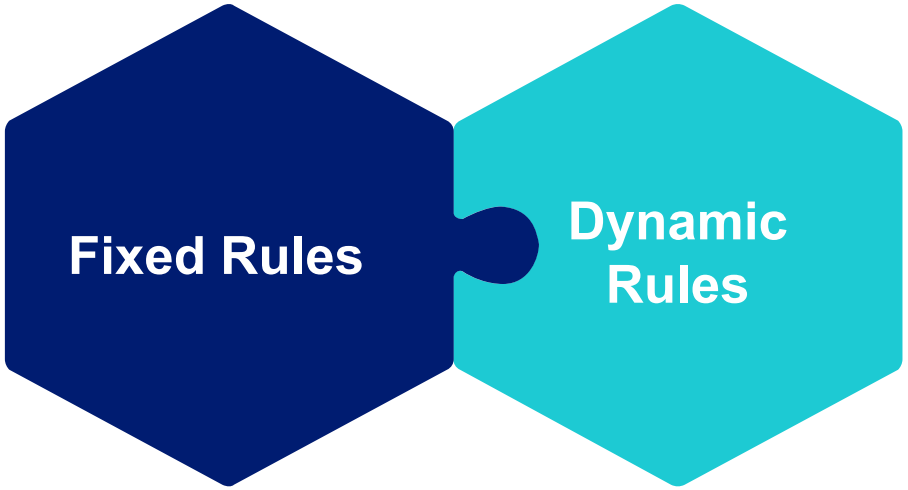


User Behavior Analytics (UBA)

We are creatures of habit



UBA software focuses on what users typically do — their activities and file access patterns. If those activities change, the system ‘knows’….



“Tell me if anyone logs in between midnight and 5:00 am”

Collect user information over time to identify patterns

Removable Media

“USBs are the Devil” — overheard at an IT Security Conference

Removable devices literally let users walk out the front door with your data!

- Disable removable media on the workstation
- Encrypt removable media if it must be used
- Keep removable media locked in storage
- Don’t allow cell phones or other picture taking devices near sensitive data

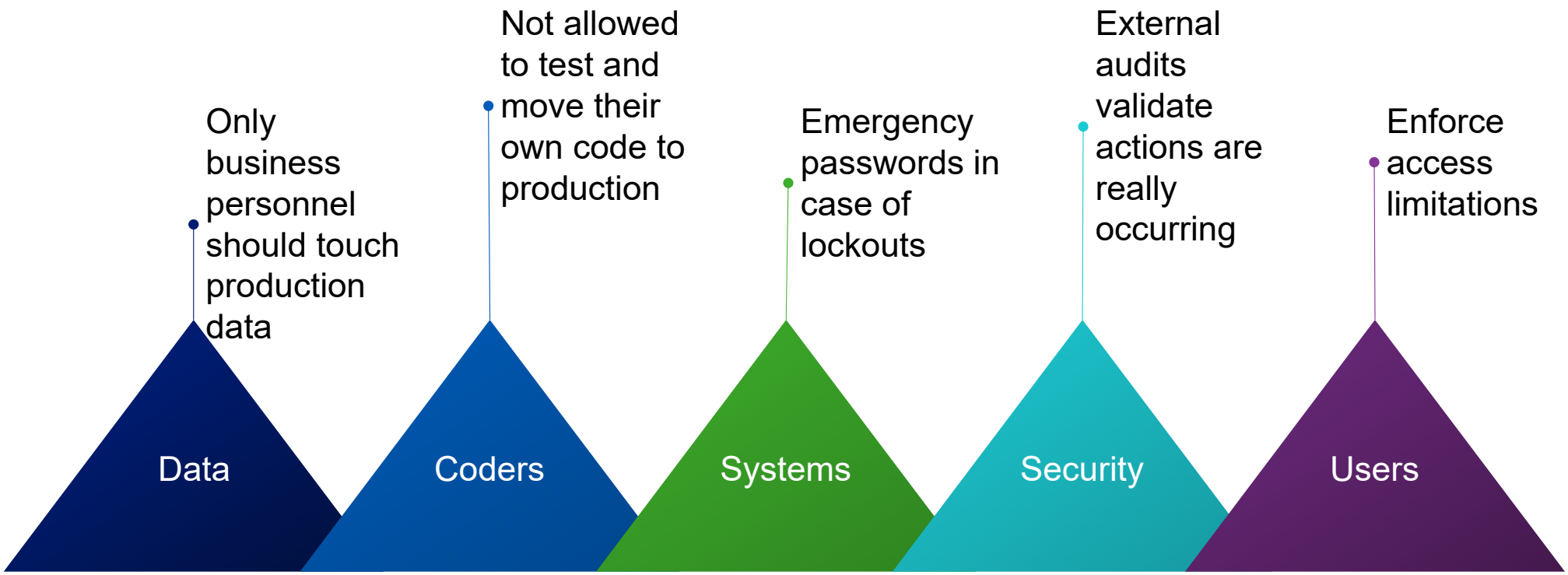
Least Necessary Access

53% of organizations found over **1,000** sensitive files accessible to **every** employee.*

- Knowing where your sensitive data is allows you to determine who can access it
- Strictly enforce a ‘need to know’ policy.

* Source: 2019 Global Data Risk Report from Varonis Data Lab from 785 Data Risk Assessments performed

Separation of Duties



Limit the ability of one person to negatively impact the confidentiality, integrity, or availability of data.

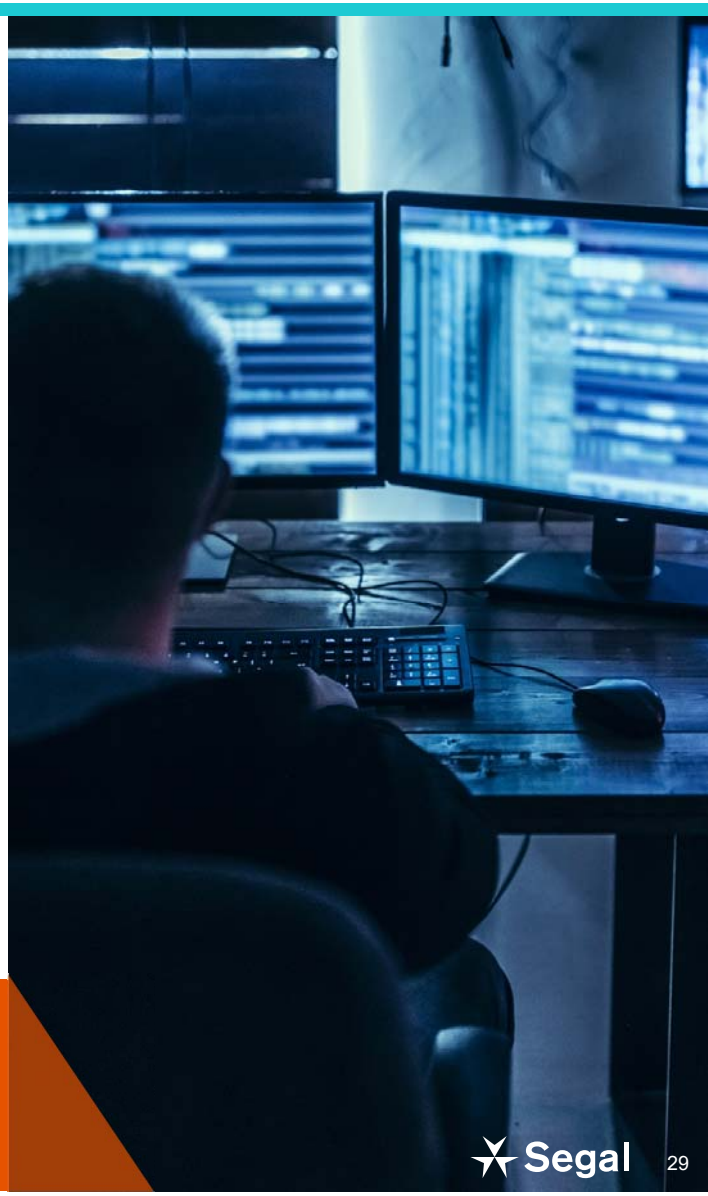
Data Surveillance

Use software alarms that let you know when someone is accessing data they are not supposed to.

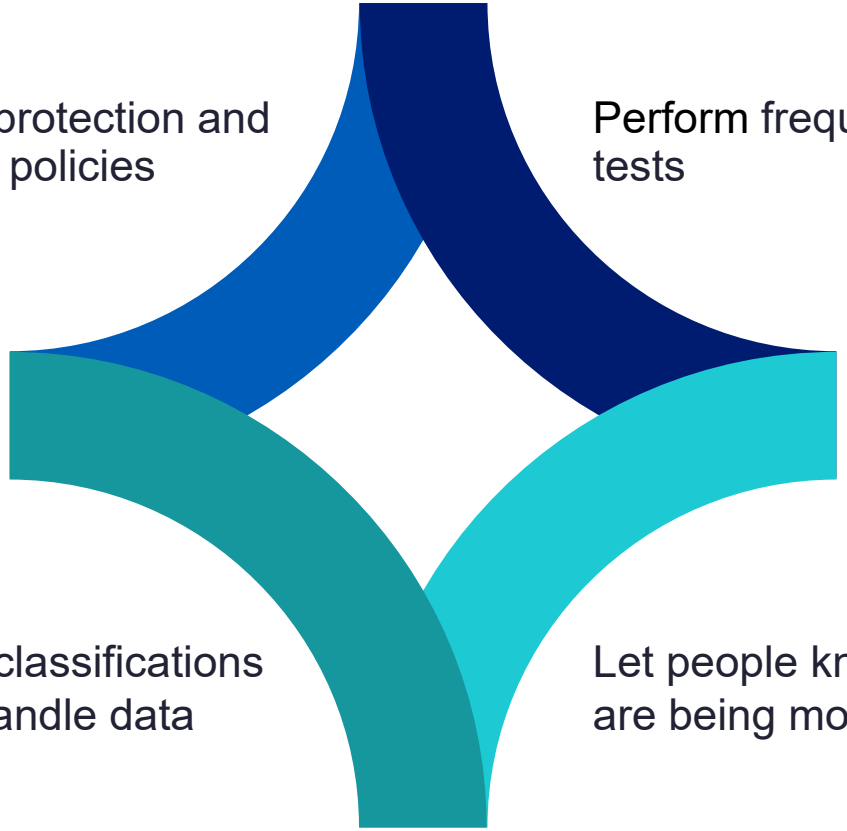
Human Resource Actions

- Perform background checks and screenings to ensure you are not hiring an insider threat
- Assure privacy and security training is conducted for new employees
- Remove previous systems access no longer needed as personnel move to different jobs
- Reset all passwords and building codes as needed after terminating an employee

July 2019 - Capital One Financial said data from about 100 million people in the United States was illegally accessed in the Amazon cloud by a former Amazon.com employee.



User Training and Awareness



Key Takeaways

- Insiders by default are ‘trusted’ and most are trustworthy … but possibly not all.
- Most insider incidents occur by accident. Use training, policies, and tools to minimize the potential for those accidents to occur.
- You are not spying on people when you monitor their work activities – you are protecting the organization from serious risks and liabilities.
- You will be hit with a cybersecurity incident eventually, whether from an insider or some other attack. You should have an Incident Response Plan ready and rehearsed when the event occurs.

Don’t become this person!

Risk Mitigation Through Insurance

In This Section…

What is Cyber Liability Insurance?

- Insurance for Ransomware Attacks
- Insurance for Social Engineering Fraud
- Key Tips for Insurance Applications
- Watching out for Cyber Exclusions

What is Cyber Liability Insurance?

Cyber insurance policies generally contain both first-party and third-party coverage. Insures against:

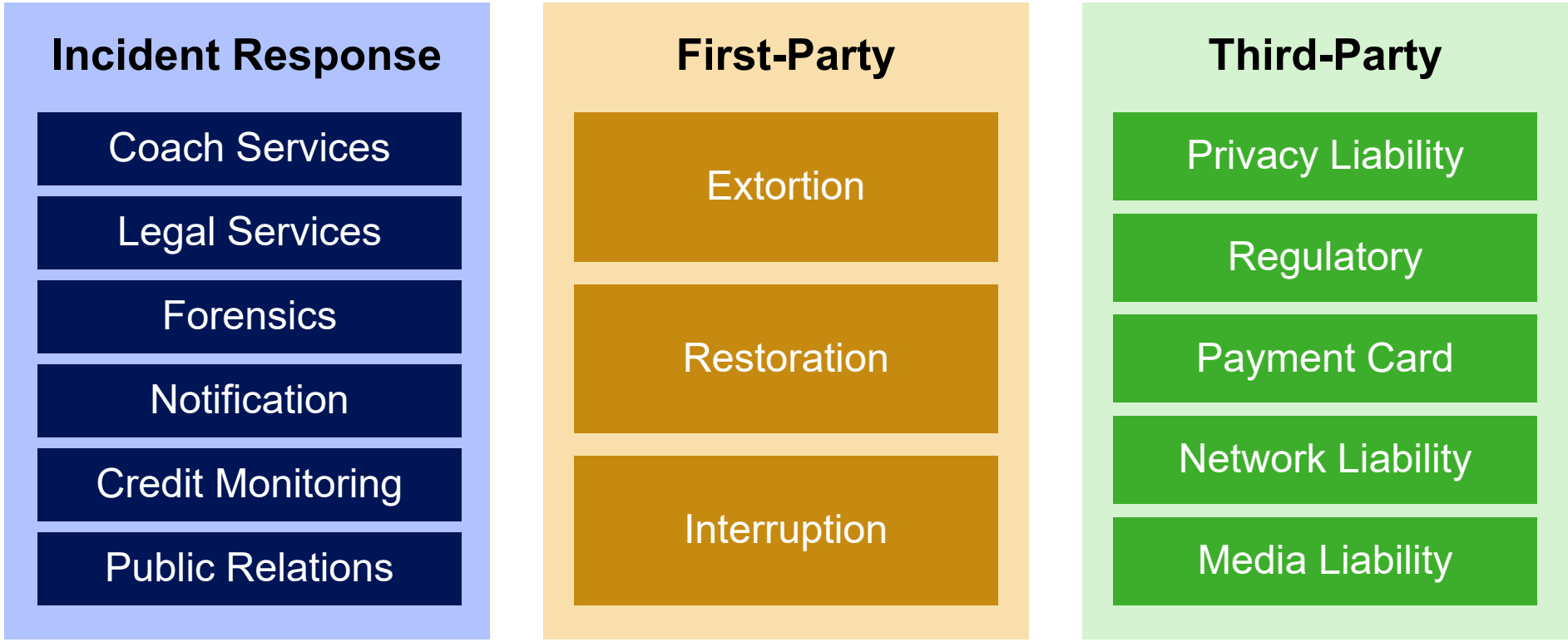
First-Party Coverage

- Insured's own losses, expenses associated with unlawful entry into their computer systems or network as well as breaches arising out lost/stolen devices
- Including the cost to notify insureds of a cyberattack or lost business income
- It should include coverage for ransom payments and extra expenses arising out of cyber extortion

Third-Party Coverage

- Liability to third-parties caused by a breach or cyberattack

Navigating a Data Breach Event



Coverage Concerns in a Remote Environment

Ransomware Attacks

- Attacks continue to increase in their frequency and in their ruthlessness
- Often let in by insiders who have been trained not to do so
- The opportunities for a successful attack have increased in the COVID environment:
  - more distributed access points such as home computers, cell phones and tables
  - fewer integrated controls on employee-owned computers
- How big of a problem?
  - Ransomware payments increased 33% to approximately $112,000 from 4Q 2019 to 1Q 2020 and the average attack triggers about 15 days of downtime

Insurance for Ransomware Attacks

Attacks are generally covered by most carriers but the extent varies:

- May employ forensic and other experts to thwart the attack in real time
- May provide professional negotiators to engage the attackers
- May pay the ransom up to a sublimit
- May provide payment via an electronic currency
- May cover extra expenses incurred during downtime to continue critical operations
- May cover damage to data or equipment as result of attack

HHS guidance: Ransomware attach is a security "incident." Certain procedures must be followed under HIPAA.

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Coverage Concerns in a Remote Environment

Social Engineering is the art of manipulating the target into providing confidential/personal information or transferring assets through:

Phishing	Pharming
Pretexting	Social Media

Decreased co-worker interaction, greater dependence on technology, increased distractions at home, and reliance on email instead of face-to-face communication with colleagues all exacerbate the problem.

Coverage Concerns in a Remote Environment

Social Engineering Fraud

- Attacks are generally covered by most carriers when malware is added, data is stolen or held hostage, or money transferred
- The coverage may have exclusions and require certain procedures to be followed in order to have a covered claim (independent call back provisions, etc.)
- If money is stolen, coverage limits are often sublimited to between $50K and $250K regardless of the full policy limit
- There may be similar coverage in other policies such as a fidelity bond
- Larger coverage limits are usually only available by having excess carriers participate in a program

Key Tips for Insurance Applications

- Who is responsible for data security?
- Are there privacy and security policies protecting confidential information?
- Has a risk assessment been conducted
- Is there an incident response plan in place?
- How many data employees have access to data?
- Is there ongoing privacy and security training?
- Are there contracts in place for 3rd parties who process, host or store sensitive information?
- What has the breach experience been and how was it handled?

Separate questionnaires are now often required to address COVID, Ransomware and Social Engineering Fraud exposures

Beware of Cyber Policy Exclusions

- Professional services
- Criminal or Intentional acts of employees
- “Failure to Follow Minimum Required Practices”
- Acts prior to the inception of the policy
- Unencrypted data exclusion
- Mechanical/electronic failure such as when a computer stops functioning
- Laptops and other portable electronics such as cell phones and tablets
- Patent, software, copyright Infringement
- War or Terrorism

Insurance Takeaways

- The threat environment has only become increasingly risky during the pandemic environment due to an increased number or remote workers and system vulnerabilities
- Ransomware attacks and Social Engineering attacks are becoming more prevalent, more expensive, and more sophisticated in their ability to trick users
- A robust Cyber Liability Insurance policy is a ‘must have’ in today’s perilous environment; ensure you have the appropriate coverage for your organization

Thank You

Contact Information

For more info, please contact us at

Christopher Nickson
Senior Consultant
cnickson@segalco.com
716.512.4366

Jay Preall
Senior Consultant
JPreall@segalco.com
636.248.7270

Mark Dobrow
Vice President, Consultant
mdobrow@segalco.com
312.984.8660