AUDITBOARD

Cyber Ransomware Attack: What Happens Next

#AuditBoardWebinars

Our Speaker

Scott Madenburg

Director, GRC Solutions Advisor

AuditBoard

- Over fifteen years of risk, audit and compliance experience.
- Experience in financial, information system, operational, and compliance auditing; Sarbanes-Oxley (SOX); business process evaluation and design; ERP system implementation and administration; mergers and acquisitions; cyber-security; and fraud investigation.
- Fox Entertainment/News Corp., Rovi Corp., Arthur Andersen.

Learning Objectives

- Learn from a breakdown of a ransom attack.
- Understand the key challenges facing organizations when a ransom attack occurs.
- Learn about post-event actions and challenges that will help define controls and processes to be considered to reduce the post-event pain.

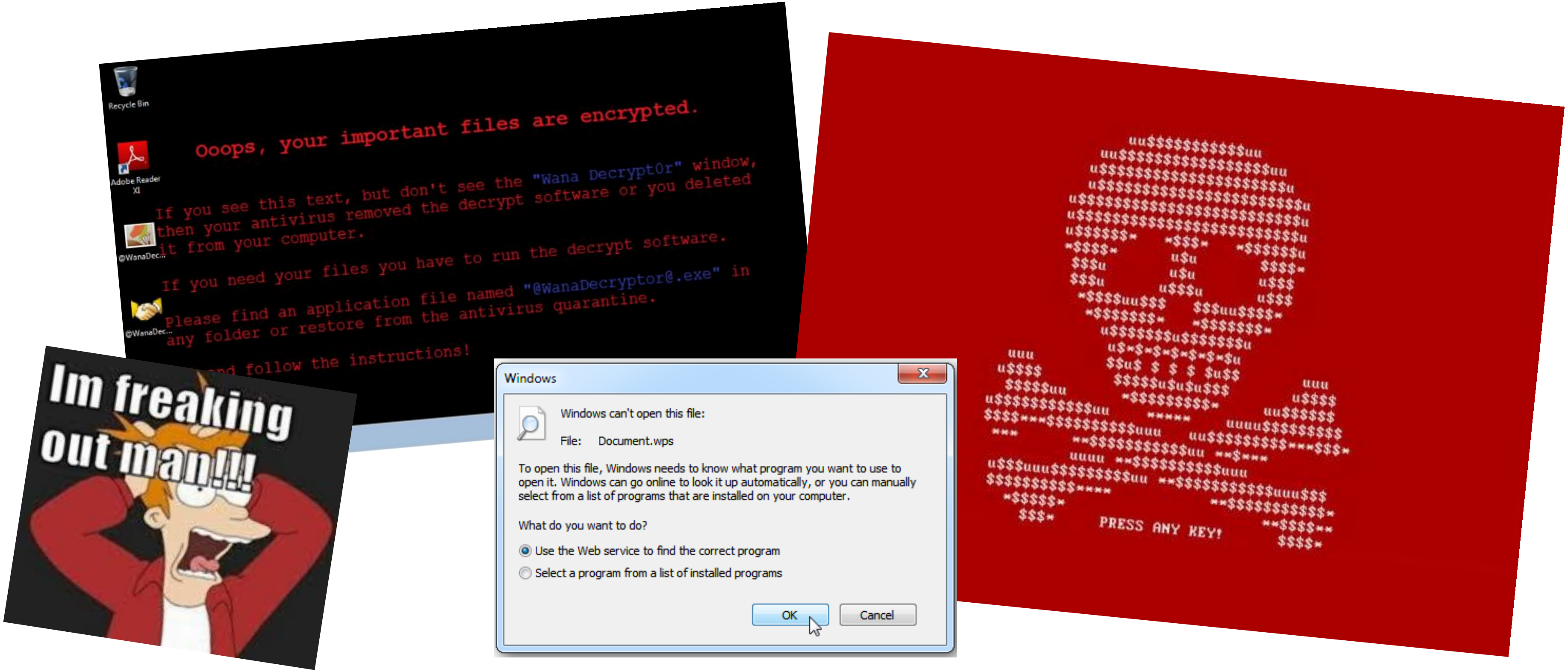
Polling Question #1

Has your company ever been the target of a cyber ransomware attack?

a. Yes.
b. No.
c. Don’t know.

Lessons Learned from a Ransom Attack

Take a Deep Breath



Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

nd follow the instructions!

Windows

Windows can't open this file:

File: Document.wps

To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

What do you want to do?

● Use the Web service to find the correct program

○ Select a program from a list of installed programs

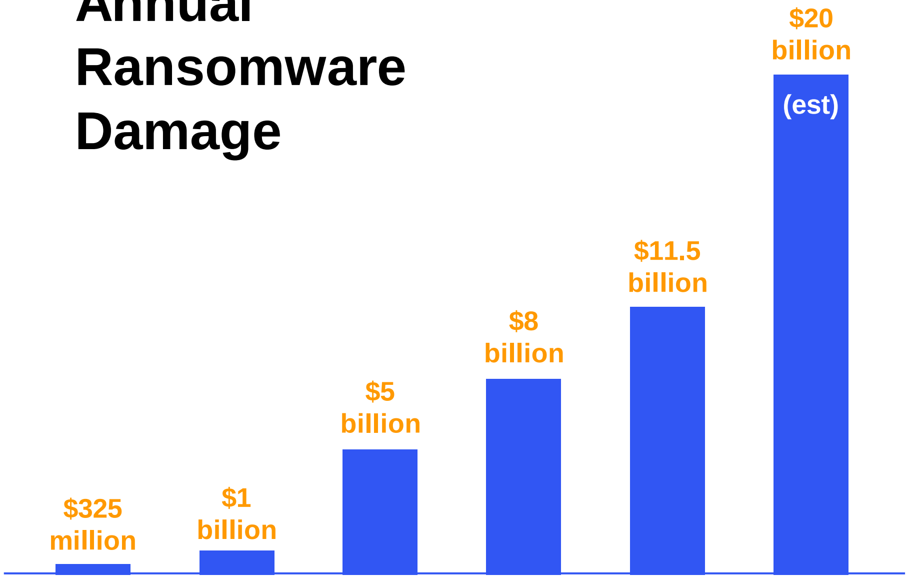
Polling Question #2

How concerned are you about the potential for your company to become the target of a cyber ransomware attack?

a. Very concerned.
b. Somewhat concerned.
c. Neither concerned or unconcerned.
d. Somewhat unconcerned.
e. Very unconcerned.

Why Be Concerned About a Cyber Ransomware Attack?

Annual Ransomware Damage



1 **365%**
Increase in business detections of ransomware from Q2 2018 to Q2 2019

2 **$10,000 to $50,000**
Increase in business detections of ransomware from Q2 2018 to Q2 2019

3 **78%**
Jump in attacks on supply chain companies

4 **14 seconds**
Predicted frequency of ransomware attacks on businesses by the end of 2019, a large jump from every 40 seconds in 2016

5 **$1 billion**
Estimated annual global revenue from ransomware attacks

6 **76%**
Percentage of organizations that believe they're likely to be victims of a malware attack in the next year

7 **55%**
More than half of those organizations don't think they would be able to findand block potential attack

What is Ransomware?

Estimated cost of ransom attacks is around $11.5 billion

Two major types: **Crypto and Locker**

- Crypto - ransomware will encrypt all the files, folders and hard drives on the infected device, promising to reinstate once a ransom has been paid to the attacker.
- Locker - ransomware simply locks users out of their devices.

Why Are Ransom Attacks Relevant Now?

- **Attack traffic is on the rise since beginning of quarantine**
  - Organizations are cutting back on headcount in this pandemic environment.
  - Working from home may demote your protection.

- **Attacks were increasing even before the pandemic hit**
  - As organizations improve their security, hackers continue to innovate.
  - Now monetizing not just data availability, but also confidentiality.

Criminals
Hacktivists
Criminal Hackers
Competitors
Foreign Nations
Disgruntled Employees

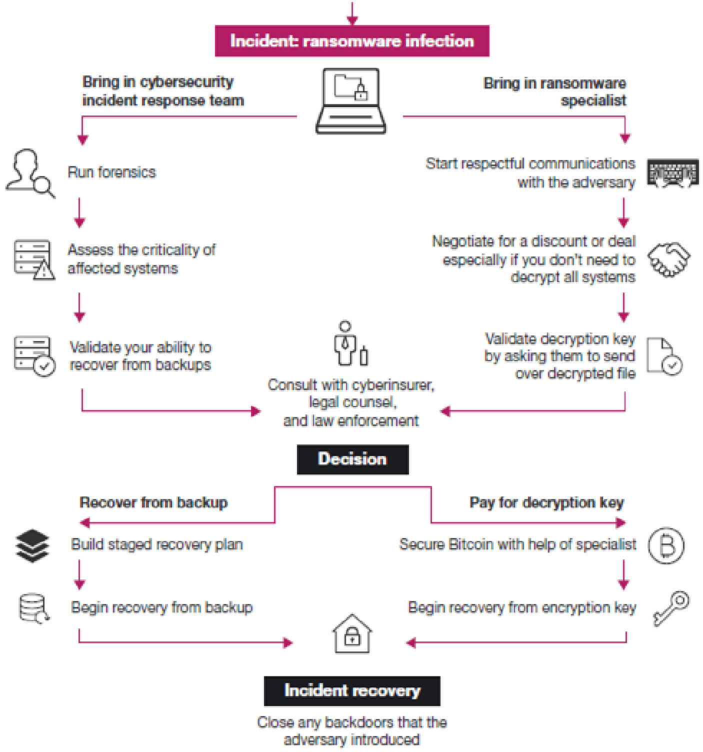
Critical Steps Following the Incident

Internal Audit's Role During the Crisis

- Usually Internal Audit assists after-the-fact, and not in real time if there is a dedicated Incident Response (IR) team.

- Audit may not play a large role in the immediate response, but this is an opportunity to learn, help review the process in real time, and make needed improvements.

What Does the Incident Response Team Think About Recovery?



Incident: ransomware infection

Bring in cybersecurity incident response team

Run forensics

Assess the criticality of affected systems

Validate your ability to recover from backups

Bring in ransomware specialist

Start respectful communications with the adversary

Negotiate for a discount or deal especially if you don't need to decrypt all systems

Validate decryption key by asking them to send over decrypted file

Consult with cyberinsurer, legal counsel, and law enforcement

Decision

Recover from backup

Build staged recovery plan

Begin recovery from backup

Pay for decryption key

Secure Bitcoin with help of specialist

Begin recovery from encryption key

Incident recovery

Close any backdoors that the adversary introduced

- Could be an in-house IR team with forensics or a third party provider.
- Containment and recovery are top of mind.
- IR tends to think about recovery in terms of:
  - Recovery point objective.
  - Recovery time objective.

Critical Steps Following the Incident

- Unplug and Inform All Employees
- Secure the Data
- Trace the Attack
- Access the Impact

- Notify the Authorities
- Notify Affected Customers
- Clean and Update Your Security Systems

Unplug and Inform All Employees

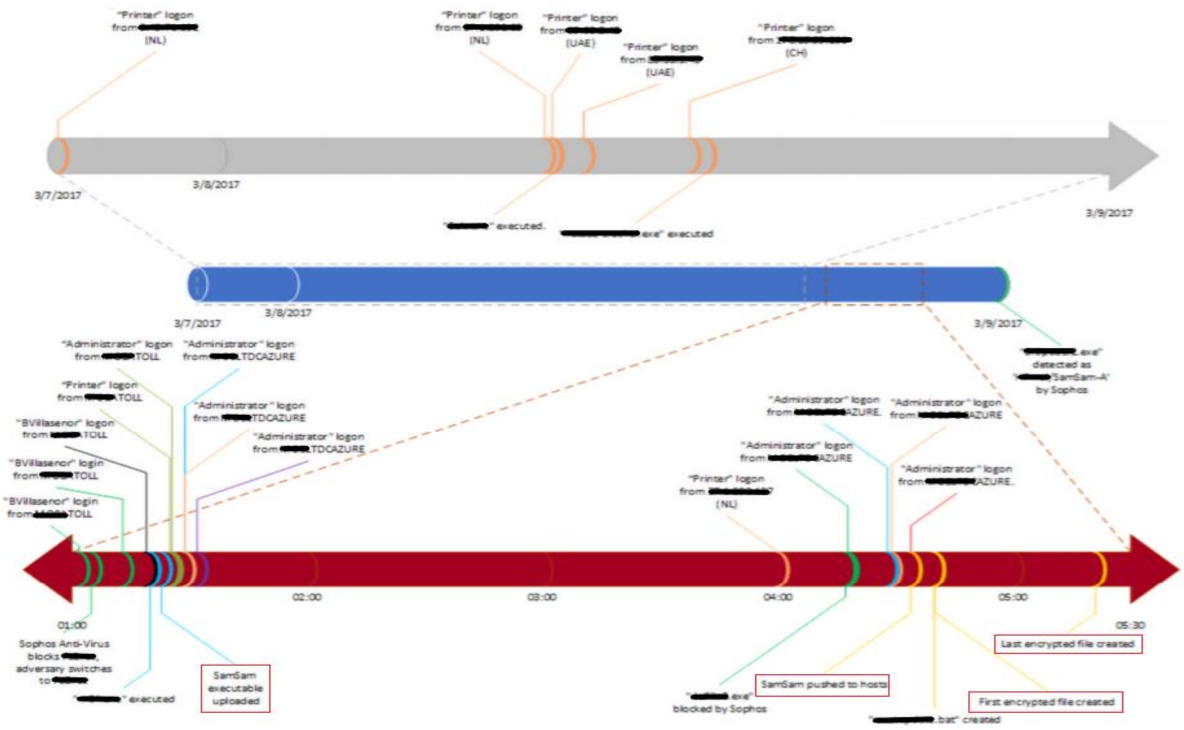
1. Do not power on, copy files, or connect to any network.
2. Read the posters.
3. Your laptop may be compromised.

Secure the Data

Take a read-only snapshot of the infected computer, virtual machine, or storage device.

Isolate or suspend a compromised section of its network temporarily or possibly even the entire network.

Trace the Attack


"Printer" logon from [redacted] (NL)
"Printer" logon from [redacted] (NL)
"Printer" logon from [redacted] (UAE)
"Printer" logon from [redacted] (UAE)
"Printer" logon from [redacted] (CH)
3/7/2017
3/8/2017
3/9/2017
"[redacted]" executed.
"[redacted].exe" executed
3/7/2017
3/8/2017
3/9/2017
"[redacted].exe" detected as "[redacted]/SamSam-A" by Sophos
"Administrator" logon from [redacted].TOLL
"Administrator" logon from [redacted].TDCAZURE
"Printer" logon from [redacted].TOLL
"Administrator" logon from [redacted].TDCAZURE
"BVillasenor" logon from [redacted].TOLL
"Administrator" logon from [redacted].TDCAZURE
"BVillasenor" login from [redacted].TOLL
"BVillasenor" login from [redacted].TOLL
"Administrator" logon from [redacted]AZURE.
"Administrator" logon from [redacted]AZURE
"Administrator" logon from [redacted]AZURE
"Administrator" logon from [redacted]AZURE.
"Printer" logon from [redacted] (NL)
01:00
02:00
03:00
04:00
05:00
05:30
Sophos Anti-Virus blocks [redacted], adversary switches to [redacted]
"[redacted]" executed
SamSam executable uploaded
"[redacted].exe" blocked by Sophos
SamSam pushed to hosts
"[redacted].bat" created
First encrypted file created
Last encrypted file created

Sample Schematic of an Attack Sequence

AUDITBOARD

Assess the Impact

Upon review of information made available and initial conversations with the client, Internal Audit may propose the following analysis efforts:

Perform host analysis on systems identified as being part of the initial intrusion.

Analyze network log data to identify ongoing or historical attacker movement within the environment.

Analyze available Domain Controller server logs to identify suspicious access activity.

Correlate relevant events to establish a timeline of malicious activity.

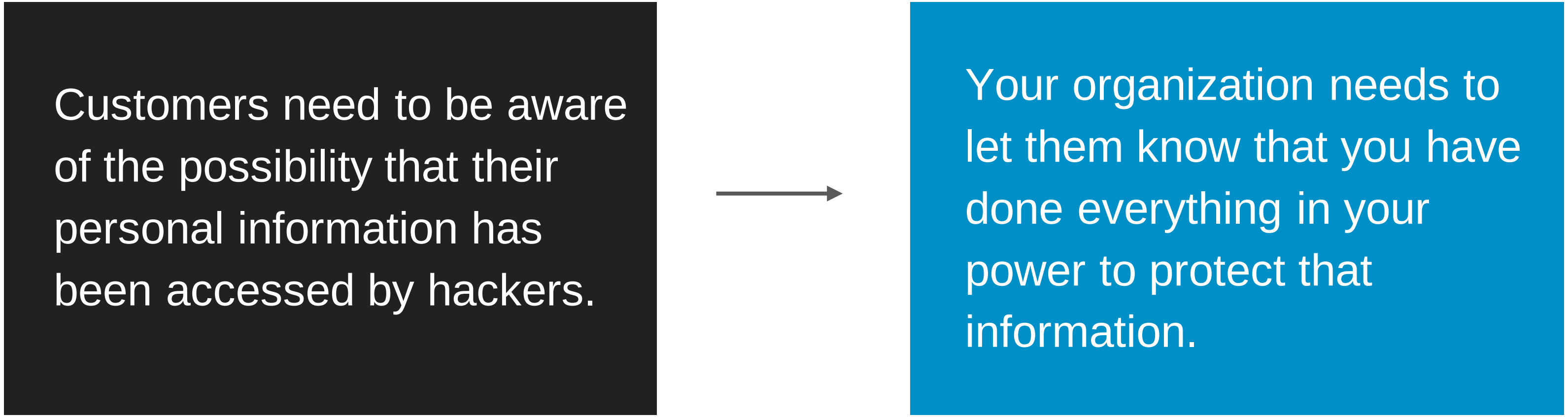
Develop recommendations based upon observations during analysis.

Notify the Authorities

- Notifying the authorities about the cyber-attack on your organization is essential to protect both your reputation and your customers.

- The FBI urges ransomware victims to report ransomware incidents regardless of the outcome. This helps the FBI to determine who is behind the attacks and how they are identifying or targeting victims.

Notify Affected Customers



Customers need to be aware of the possibility that their personal information has been accessed by hackers.

Your organization needs to let them know that you have done everything in your power to protect that information.

Clean and Update Your Security Systems

After the incident is over, you'll need to perform a total security audit and update all systems.

Malware should be securely removed, systems should again be hardened and patched, and updates should be applied.

Questions to address:

- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened and patched, and have updates been applied?
- Can the system be re-imaged?

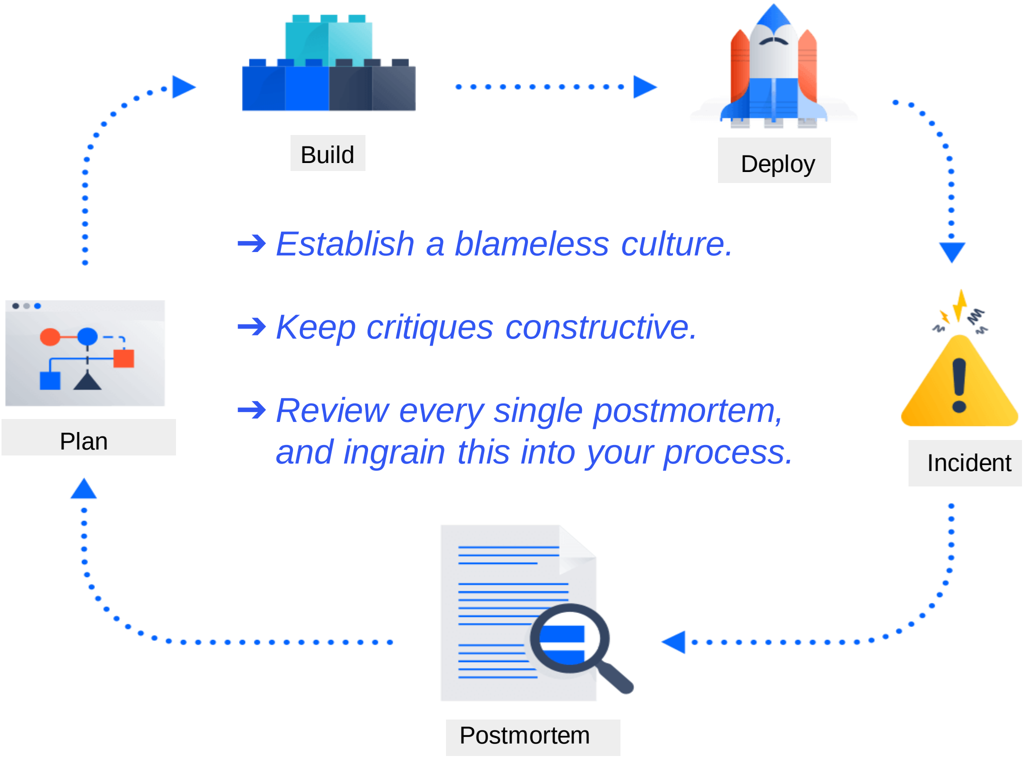
Polling Question #3

Does your company have a plan to address a cyber ransomware attack if one occurs?

a. Yes.
b. No.
c. Don’t know.

Post-Event Actions

Conduct a Postmortem



- ➔ *Establish a blameless culture.*
- ➔ *Keep critiques constructive.*
- ➔ *Review every single postmortem, and ingrain this into your process.*

Bringing people together to engage in a structured, collaborative process allows everyone to contribute what they learned and can build trust and resiliency within your team.

Documenting the incident and how the team remedied it can inform how future incidents are handled.

Internal Audit’s Role After the Incident

IR team can note which business units had the most severe incidents. Internal Audit can audit these areas and test controls linked to root causes.

- **More valuable audits for being applicable to real-world risk**

- **Tie outcomes of these audits to real cost or show reduction of risk and incidents**

- **Auditees more willing to participate in good faith, a lower risk way to address issues vs the high-stress experience of an actual attack**

Considerations

1 Practice good cyber hygiene: backup, update, whitelist apps, limit privilege, and use multi-factor authentication (MFA).

2 Segment your networks: make it hard for the bad guy to move around and infect multiple systems.

3 Develop containment strategies: if bad guys get in, make it hard for them to get data out.

4 Know your system's baseline for recovery.

5 Review disaster recovery procedures and validate goals with executives.

6 Ensure insurance coverage is appropriate.

Polling Question #4

Are you incorporating any of the following considerations in your audit plan? (select all that apply)

a. Practice good cyber hygiene: backup, update, whitelist apps, limit privilege, and use multi-factor authentication (MFA).
b. Segment your networks: make it hard for the bad guy to move around and infect multiple systems.
c. Develop containment strategies: if bad guys get in, make it hard for them to get data out.
d. Review disaster recovery procedures and validate goals with executives.
e. Ensure insurance coverage is appropriate.
f. None of the above.

Key Challenges

Challenge: Incident Response Data

Challenge

Nothing happens with the incident response data.

Response

- Use incident data to reduce risk, and drive prioritization and strategic decision-making.
- Make it part of your ERM process.

Challenge: Control Library

Challenge

Incomplete control library.

Response

Having a holistic risk and control library.

Challenge: Materiality

Challenge

Not thinking about the materiality.

Response

Correlate number or dollars lost per incident and map to control areas, then audit controls in areas that led to highest number of incident failures.

Final Thoughts: What’s Next?

Cyber Ransomware Attacks are on the Rise

Pervasiveness of remote work resulting from the pandemic is making more companies vulnerable to cybercrime. According to VMWare, there has been a 148% increase in ransomware attacks.

- ➔ A remote IT team makes recovery more difficult.
- ➔ A remote workforce makes it harder to enforce security protocols and increases the risk of attack.

Preventative Roles for Internal Audit

- Develop a mapping of what key control areas map to the threats that you worry about.

- If you expect ransomware to be a big threat either because there are many in your industry or you've had the experience, then you can point audits at those areas.

- Conduct surveys or interview-based discussions to identify top threats, map controls to each threat, and assess each control.

- Spend more time in these areas because they map to the most plausible threats that the business faces.

AUDITBOARD

Q&A

AUDITBOARD

Thank You!