Thank you for joining us today

WE WILL START MOMENTARILY

MAYNARDNEXSEN

XANTRION
TECH EXPERTS, ENDURING PARTNERS

Before we get started…

WE RESPECT YOUR TIME:

We will not run more than 60 minutes!

QUESTIONS ARE ENCOURAGED:

Please submit using Q&A feature, not chat. We'll answer questions at the end of the presentation.

BEST VIEWING OPTIONS:

Gallery view & under more options, select full screen & hide me

RECORDED PRESENTATION WILL BE SENT NEXT WEEK

CYBERSECURITY ASSESSMENTS:

Why Your Company Needs One and Where to Start

MAYNARDNEXSEN

XANTRION
TECH EXPERTS, ENDURING PARTNERS

Moderator: Heather Hoopes-Matthews

Heather Hoopes-Matthews

CEO, NP Strategy

Heather is an award-winning journalist and host of *Taking the Pulse* podcast. With a passion for turning complicated topics and issues into clear and concise points, Heather specializes in messaging and stakeholder engagement in rapidly changing environments. After many years as an investigative reporter, Heather launched NP Strategy where she develops and implements community relations efforts for economic development projects and trains executives and government officials on public speaking and media relations.

Panelist: Brandon Robinson

Brandon Robinson

Shareholder, Maynard Nexsen

Brandon is an attorney in Maynard Nexsen's Cybersecurity & Privacy group and is CIPP/US and CIPP/E certified. He provides data security and privacy counseling to companies across multiple industry sectors, helping them to ensure compliance with the quickly evolving legal and regulatory landscape of privacy and cybersecurity. His team's counsel spans the entire lifecycle of a company's data, including both proactive measures – designed to comply with laws and regulations, allocate risk, and prevent incidents – and reactive measures in the event a security incident occurs.

Panelist: Darren Nyberg, VP of Client Strategy, Xantrion

Darren Nyberg

VP of Client Strategy, Xantrion

After 17 years of helping small and medium businesses navigate the rapidly evolving IT landscape, Darren now leads the strategic advisor team at Xantrion, an award-winning Managed Service Provider. The team's mission is to enable clients to thrive in the face of regulatory and digital disruption. Their proven cyber assessment methodology helps clients not only stay one step ahead of bad actors, but also guides their IT strategy and investment. With the right partner and methodology, assessments are and not just a mere report, but blueprints for success.

What is a cybersecurity assessment?

A cybersecurity assessment is a comprehensive review of an enterprise's cybersecurity program and its risks and vulnerabilities.

An assessment can help inform an organization's decisions on where to invest its resources to reduce cyber risks and improve its cybersecurity profile.

An assessment should cover top IT controls, including:

- Logical access policies and procedures
- Data backup and recovery procedures
- Incident management policies and procedures

Why do companies get cybersecurity assessments?

Proactive reasons for cybersecurity assessments:

- ➔ Cyberthreats are rapidly evolving in sophistication and frequency, which means it's incumbent on every organization to be proactive on cybersecurity readiness.
- ➔ Increasing use of different cloud-based platforms & the necessity of understanding the risks of each
- ➔ Improving company policies and procedures for better employee alignment

Reactive reasons for cybersecurity assessments:

- ➔ Statutory / Regulatory requirements
- ➔ Investor or customer pressure
- ➔ Suffered a costly breach & determined to avoid future ones

Average breach cost for US SMBs **$3.31 M**

Source: 2023 IBM Study

High levels of planning reduce breach cost by about **50%**

Source: 2023 IBM Study

What are the different types of cybersecurity assessments?

Self-Assessments i.e. online surveys

- ➔ The person completing the survey often has inaccurate or outdated information and provides answers that are more favorable than reality

Automated Scans

- ➔ Scans typically provide incomplete information i.e. don't account for cloud-based data and applications

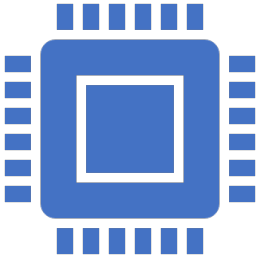
Third-Party Reports from Relevant Experts – IDEAL METHODOLOGY

- ➔ Assessments by managed services providers like Xantrion primarily assess your technical cybersecurity risks and how to mitigate key risks with technology
- ➔ Assessments by law firms with cybersecurity expertise like Maynard Nexsen assess your compliance risks and quality of written policies
- ➔ Ideal assessment is one where legal and technical experts work together to conduct a comprehensive assessment that holistically addresses the use and governance of technology and information.

How are cybersecurity assessments structured?

Cybersecurity assessments are typically based on frameworks that provide a common language for understanding cyber best practices and how to reduce cybersecurity risks.

The most widely used and well-known framework comes from the National Institute of Standards and Technology or NIST.



Xantrion bases its cybersecurity assessment on the NIST framework while also drawing from other frameworks and incorporating additional aspects from Xantrion's decades of experience.

Case Study: Registered Investment Advisor (RIA)

Background

- 60- person RIA with $13.5 billon in Assets Under Management

Assessment Driver

- Keeping current with evolving regulations and cyber threats

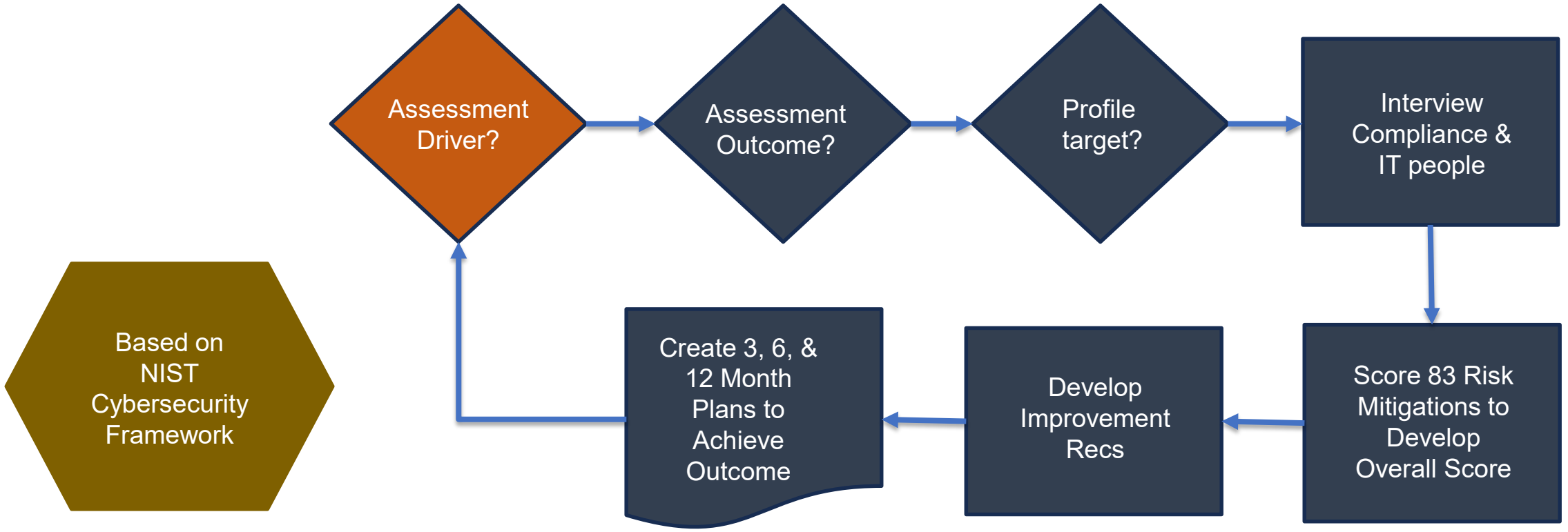
Desired Outcome

- Target security risk profile 1

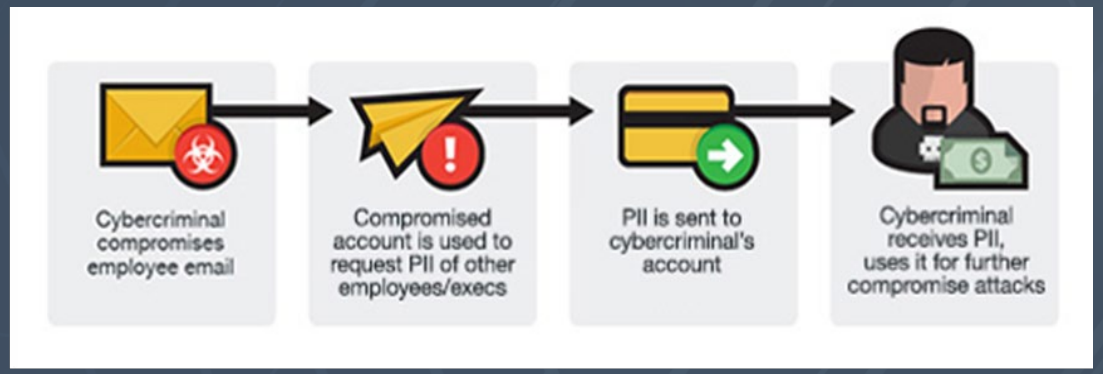
Assessment Takeaways

- Technical protections were sound
- Significant gaps around missing policies, such as a Business Continuity or Incident Response policies, and a lack of annual policy reviews
- Assessments should be regular to update policies, keep current with evolving threats and technology and reduce risks

Registered Investment Advisor Case Study



Case Study: Business Email Compromise ("BEC")



INDUSTRY: **Small manufacturing facility**

CHALLENGE:

- Facility received email from vendor to change routing information for payment of multiple invoices. Facility transferred the funds per instructions.
- Months later, when vendor inquired as to why they had not been paid, it was discovered that vendor email account had been compromised and instructions were fraudulent.
- By that time, the money was gone, and too late for FBI/SS/law enforcement to recover the funds.
- Facility and vendor now must negotiate/litigate on who bears the risk of loss.

LESSONS

- This could have been avoided if improved policies and procedures were adopted and implemented. (e.g., telephone confirmation, MFA, etc.)
- Such measures could prevent occurrences whether due to phishing attacks (bottom picture) or actual system compromise (top picture) as was the case here.

Case Study: Business Email Compromise ("BEC")

LESSONS

- This is increasingly common. 70% of organizations were targets of BEC attacks in 2023; 29% of those were victims of 1 or more successful BEC attacks. (Arctic Wolf, 2024).
- Roughly 88% to 95% of Data Breaches are caused by human error - an employee mistake (Stanford/Tessian, 2020; IBM 2014).
- Losses from mistakes such as these are direct and calculable.
- A comprehensive cybersecurity risk assessment would have identified this vulnerability (and others) and recommended changes to avoid such issues in the future.

Takeaways

- Assessments inform an organization's decisions on where to invest its resources to reduce cyber risks and improve its cybersecurity profile
- Consider conducting assessments before an incident occurs to significantly reduce the likelihood and cost of an incident
- 3rd party reports by relevant experts working together are the best way to get a comprehensive, accurate assessment of your risks and the best way to mitigate them
- Use a standard assessment framework methodology that provides a common language for understanding cyber best practices and how to reduce cybersecurity risks
- Perform assessments regularly to continue to reduce cyber risk and keep current with evolving landscape
- The fastest way to get started with a cyber assessment is to consult your IT, legal and compliance team and bring in relevant experts if needed to augment team experience

Please submit questions via Q&A feature