What CEOs Need to Know Now About Cybersecurity

Jim Tiller
CISO
Nash Squared and Harvey Nash

ASA ExecuVision

Cyber Challenges

THREATS

- Ransomware
- Cybercriminals
- Deepfake/AI
- Cyberwar & Nation State
- Zero-Day
- Advanced Hybrid Threats

TRANSFORMATIONAL

- AI
- Cloud
- IoT/OT
- Zero Trust
- Mobility
- Automation

OPERATIONAL

- Supply Chain
- Cyber Skill Shortage
- Incident Response
- Cyber Culture
- Cyber Insurance
- Compliance

Changing Realities of Cybersecurity

PSYCHOLOGICAL IMPACT

- **Overwhelming**
  - Everything from every direction
  - Risk difficult to identify, much less characterize
  - Analysis paralysis, everything is critical
  - Seemingly endless budget demands without clarity on effectiveness or outcomes
  - Who to trust?

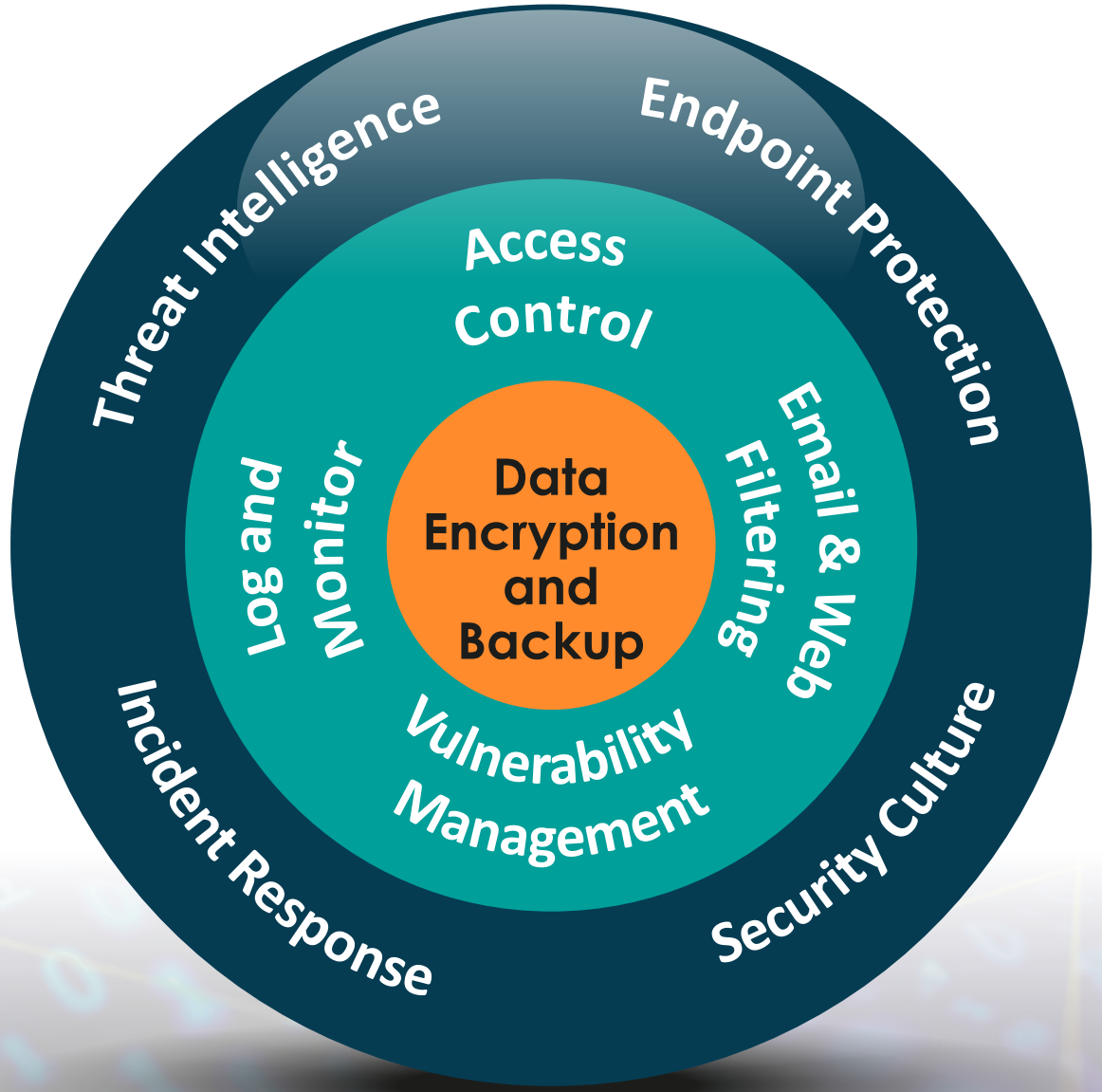
EVOLVING PERSPECTIVES

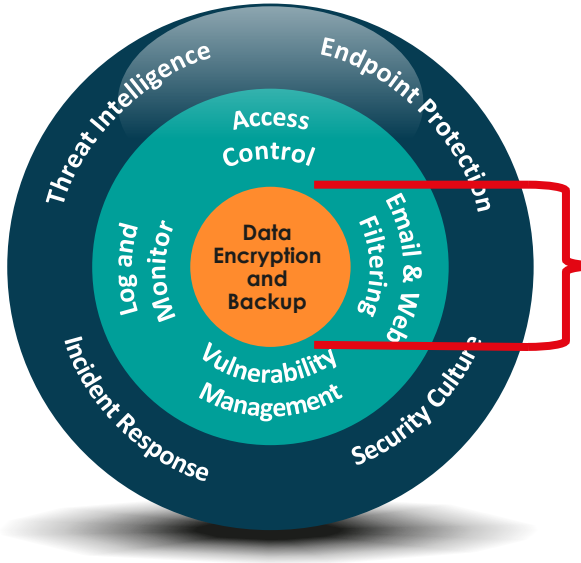
Was…	Now…
It's not **IF**, but **WHEN**	It's how you **RESPOND**
Defense Posture	**Resilience** Posture
Tactical point solutions targeted at **specific needs**	**Strategic** approach driven by **equitable interlocks**
CIA "Confidentiality, Integrity and Availability"	**DIE** "Distributed, Immutable, and Ephemeral"

Focus on the Basics

PERSISTENCE WINS THE WAR

- **A Journey, not a Destination, But it doesn't have to be uphill.**
  - Being Pragmatic and Practical
  - A lot of little steps are better than a single big one
  - Know your environment and your enemy





Data

It's difficult to isolate "critical and valuable" information assets in today's business environment, but in virtually all cases, you can encrypt data in storage and in transit.

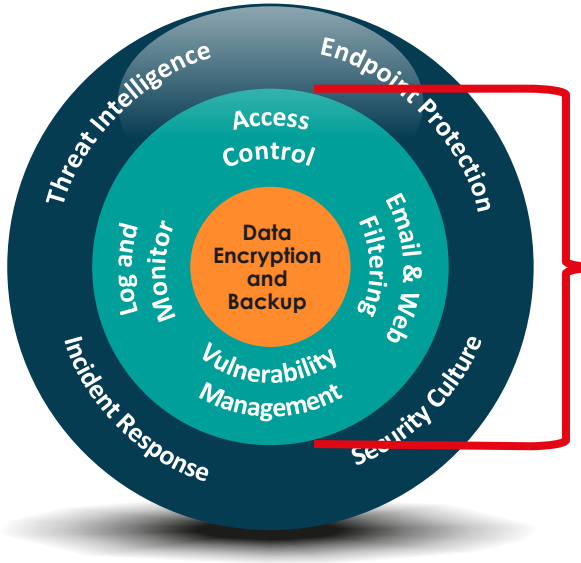
Guidance

- Endpoint **hard drive encryption** (Bitlocker FileVault)
- **Removable storage** devices encryption
- **Cloud** container encryption
- Use **VPNs** in every possible case, and encourage for personal use with employees

---

Sophisticated approaches to backing up data and protecting backups is critical to being resilient

- Having Box, OneDrive, Google Drive, or a secondary S3 container **doesn't entirely qualify as a backup**
- **Secure backup media** and have several versions
- **3-2-1 Rule**
  - 3 copies of your data
  - 2 different storage media
  - 1 copy is kept off site



Access Control

Controlling access is where most mistakes happen. Weak or password reuse is one of the most significant cyber issues

Guidance

- **Implement MFA** for everything – period
- **Password reuse is more dangerous** than weak passwords
- **Explore passwordless options**, facial recognition, and FIDO technologies to reduce reliance on passwords
- Explore YubiKeys for critical accounts

Email and Web

Most attacks are perpetrated through email and web-based threats that exploit human interpretation (think "magician")

- Aggressive **email filtering**, especially inbound attachments
- Look at solutions that "detonate" attachments or other forms of potential malware
- Utilize third party services for **web filtering and DNS security**

Vulnerability Mgt.

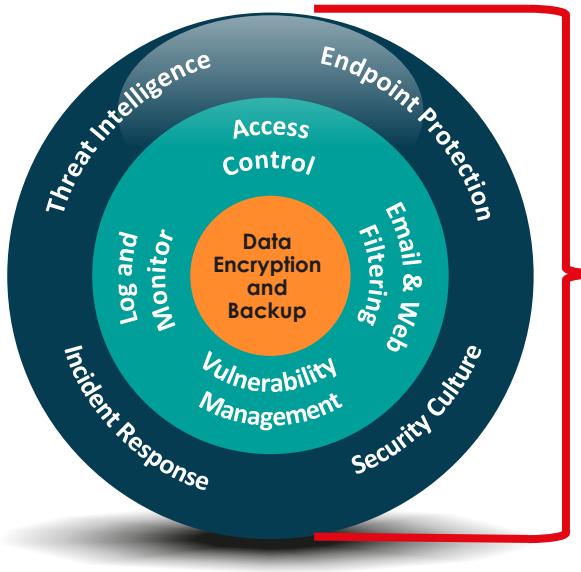
Meaningful oversight of even the most basic vulnerabilities can dramatically improve resistance to attack

- Ensure confidence that you're seeing your **entire infrastructure** in pursuit of vulnerabilities
- Collect and process information about vulnerabilities that exist within your environment and **prioritize**, especially with vulnerabilities with known exploits
- Establish and execute a plan that **tracks the entire vulnerability lifecycle** within the environment
- Regularly perform a **well-defined and planned** penetration test

Monitoring

Continuous monitoring of the environment is essential to understand the state of controls as well as potentially threatening activities

- Collect information from **key systems**, despite the ability to collect everything
- Regularly **monitor** and check for **key indicators** that relate to specific threats or specific attributes about your environment and business



Endpoint Protection

Establishing meaningful security controls at every point that interacts with your business is critical

Guidance

- **Implement EDR** (Endpoint Detection and Response) on all devices
- Be especially focused on detection and automated remediation
- Be very careful of "whitelisted" programs, especially those for temporary use
- Do not let the other practices waver because of the promise of EDR

Security Culture

Never underestimate the power of your team. Making security meaningful to them as an individual and to their families is enormously valuable to a company

Guidance

- Security **training for compliance**, while needed, has proven to be completely **ineffective**
- Make cybersecurity **valuable to the individual** and both company and employee will benefit
- Well-designed **gamification** for employee engagement has proven highly effective

Incident Management

The effectiveness of planning on how to respond in a wide range of attack scenarios has a direct correlation to financial and reputational damages

Guidance

- If nothing else, establish a **communication plan** with all key business representatives
- **Test the plan** regularly with everything from short zoom meetings to well-formed table-top exercises
- Always **keep the plan updated**
- Consider leadership training on **Crisis Management**

Threat Intelligence

Knowing is half the battle. Albeit "scary" insights, knowledge is power in cybersecurity and it will save you from poorly aligned security investments

Guidance

- Minimally, obtain information concerning **actively exploited vulnerabilities** (CISA's Known Exploited Vulnerabilities Catalog)
- Obtain threat intelligence on baseline activities, such as malware, targeted environments, and targeted industries
- Compare discovered vulnerabilities with **CVSS scoring and MITRE Att&ck framework**

When in Doubt…

FOCUS ON

- Vulnerabilities are just that, **manage them**
- You can't fight what you can't see, **monitor**
- There are no walls in the 21st Century, **endpoint security** is critical
- Backup everything and often, storage is cheap compared to the **expense of the data**
- Comprehensively **control access,** assume no trust and remove when not needed
- Make cybersecurity valuable to your employees as people, **everyone wins**
- Seek ongoing professional guidance, vCISO

Thank you.

Jim Tiller
N²: Chief Information Security Officer
Jim.Tiller@nashsquared.com