KPMG

HIMSS
New England Chapter

Healthcare Cybersecurity – Where we go from here…

Michael Thompson

November 2017

Agenda

Healthcare and cybersecurity – The target on our back

Evolving threat landscape – Where are the bad guys strong? Where are we weak?

KPMG's viewpoint – What can we do about it?

Healthcare and cybersecurity – The target on our back

Why Healthcare companies are big targets

High value of PHI records, medical ID theft, etc.

Escalating complexity and risk for data and technologies to support new and differing identities (EMR Interoperability) introduced into corporate ecosystem

Emergence of shared services and outsourcing along with cloud enabled business solutions will increase risks and opportunities for sensitive data loss

Sensitive data loss

Healthcare systems often require outdated legacy systems to support IT and OT infrastructures. Sensitive medical devices difficult to monitor & maintain

Sensitive, time-critical operations leave little tolerance for issues and interruptions, making ransomware and out-of-date systems a larger threat than other industries

Value of Healthcare Data

Patient/member information is easy to obtain and has a high resale value:

- A stolen medical identity has a $50-$365 street value (more effort to obtain)
- Stolen social security number or credit card number only sells for $1 (high volume available, easy to detect and stop use)
- Medical ID theft occurs when one person steals another's medical information to obtain or pay for healthcare treatment. Medical identity theft has affected 1.5 million Americans at a cost of more than $30 billion (World Privacy Foundation).
- Avi Rubin, Director of the Johns Hopkins University Health and Medical Security Lab, said the healthcare sector was the "absolute worst" in terms of cybersecurity.
- "Malicious actors want as much intelligence as they can get, and healthcare is the easiest attack surface for seasoned and non-seasoned hackers." (James Scott, co-founder and senior fellow at the Institute for Critical Infrastructure Technology (ICIT) in Washington D.C.)

The number of medical identity theft victims in the United States has increased from 1.42 million in 2010 to 1.85 million in 2012 and healthcare fraud, which almost always requires medical identity theft to commit the fraud, costs the United States at least $80 billion a year. Medical identity theft and fraud is much more complex and difficult to mitigate than the much more publicly known financial identity theft and fraud. Because criminals can monetize medical identities 20 to 50 times better than a financial identity, the value of a medical identity can be up to 50 times greater than a Social Security number alone. The high value of medical identities motivates criminals to put more effort in illegally attaining medical identities resulting in more and more cases of medical identity theft. As more and more PHI is being converted from paper health records to electronic health records (EHR) to improve information sharing and accessibility, the PHI becomes increasingly vulnerable to data breaches.

MIFA
MEDICAL IDENTITY FRAUD ALLIANCE

Security Threats of the “Old Normal”

- Compliance was the main focus of our Information Security program
- As an industry, we have been more focused on ease of use and audits than attackers getting our data
- IT departments and functions only engaged security teams when they thought there might be an implication to these regulations
- Today, our world has changed…

Evolving threat landscape –

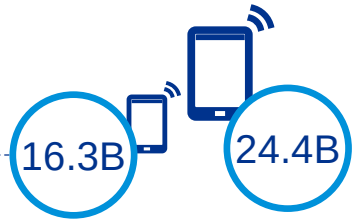
Where are the bad guys strong? Where are we weak?

New platforms mean new threats

More users
3.0 billion in 2015
4.0 billion in 2018

More smartphone connections
3.3 billion in 2015
5.9 billion in 2020

More data
8.8 zettabytes in 2015
44.0 zettabytes in 2020



More IP-connected devices
16.3 billion in 2015
24.4 billion in 2019

More network traffic
72.4 exabytes per month in IP traffic in 2015
168.0 exabytes per month in IP traffic in 2019

Who is doing it?

Cyber threats are malicious activities carried out via digital means.

There are generally 5 types of attackers:

THE INDIVIDUAL

— Motivated by revenge, notoriety, or profit. Can be either an individual external to the organization or within it.

ORGANIZED CRIME

— Motivated solely by financial gain.

NATION – STATE

— Motivated by improving geopolitical position or commercial interests.

HACKTIVISTS

— Goals include attacking or disrupting to further a political agenda.

CYBER TERRORISTS

— Goals include destroying critical infrastructure to further a political agenda.

Current cybersecurity landscape

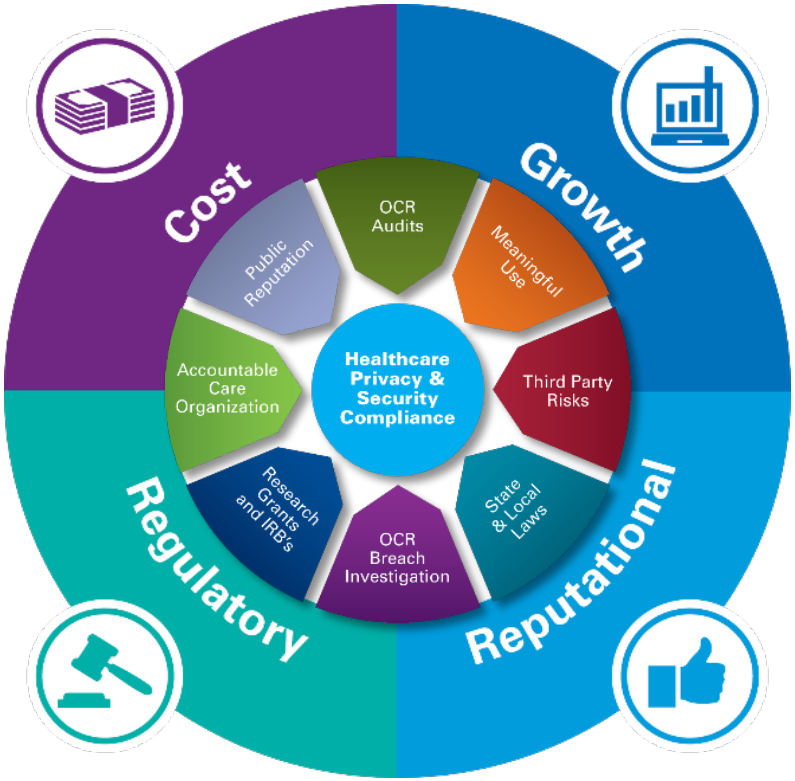
Adversaries are getting more advanced

The number of endpoints and the amount of sensitive data that needs to be protected is **exponentially increasing**

The business continues to grow into new digital businesses in**creasing pressure on IT and security**

New cyber regulations continue to challenge organizational focus

Cyber spend is reducing as cyber fatigue sets with the board, which is focused on the reduction of cyber and reputational risk



Recent events and breaches

- Healthcare and life sciences organizations are increasingly targeted by malicious attacks
- Hacker incidents account for almost half of the breaches added to the HHS list of breaches affecting 500 or more individuals during 2017
- Ransomware, social engineering and insider threats continue to be troublesome
- Phishing/hacking nets nearly $3MM from six healthcare entities [1]
- 400 hospitals' billings were delayed as clearinghouse was hit with ransomware [1]
- In 2016 Ariad Pharmaceuticals was the victim of a sophisticated social engineering attack, resulting in the disclosure of personal information of employees [2]
- Five people, including two research scientists, were indicated on charges of stealing trade secrets from GlaxoSmithKline [3]
- Johnson & Johnson announced a security vulnerability in insulin pumps that a hacker could exploit to overdose diabetic patients with insulin [4]

Sources: [1] http://www.healthcareinfosecurity.com/healthcare-hacker-attack-victim-tally-soaring, Marianne Kolbasuk McGee (HealthInfoSec) August 25, 2016
A CHIME Leadership Education and Development Forum in collaboration with iHT2
[2] New Hampshire Department of Justice http://www.doj.nh.gov/consumer/security-breaches/
[3] https://www.nytimes.com/2016/01/21/business/5-accused-of-stealing-drug-secrets-from-glaxosmithkline.html?_r=0
[40 http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L

KPMG

Landscape focus: Ransomware

Ransomware in Healthcare

- Ransomware attempts increased 4X in 2016 relative to 2015 and expected to double again in 2017 vs. 2016 (SC Magazine)
- 40% of spam email contained ransomware (IBM)
- Healthcare and Financial Services hardest hit Industries due to their dependence on business-critical information (Malwarebytes)
- Ransomware is increasing in popularity and complexity due to its ease of use and profitability for hackers.
- According to a new Healthcare IT News and HIMSS Analytics Quick HIT Survey, about 50% of all hospitals that responded said they suffered from a ransomware attack. Another 25% said they were unsure or had no way of knowing.
- Most business face at least 2 days of downtime but less than 25% of victims actually report it (the Atlantic)

Ransomware – What is it?

Ransomware is a type of malware that encrypts an entire computer or system and demands a ransom payment in exchange for the encryption key.

- Spread through common virus vectors
  - Malicious links in phishing e-mails
  - Downloads from malicious sites
  - Self-propagating worm viruses
- Can affect data via loss or operation via disruption – Also possibly data theft
- Ransom is commonly relatively low for corporations though rising

Recent global event - WannaCry

Virus name: WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY, Externalblue

Affected systems: Windows – Vista SP2, Windows 2008 R2, Windows 7, Windows 8.1, Windows 2012 R2, Windows 10, Windows Server 2016 (other Windows versions affected by ETERNALBLUE may be vulnerable – see below)

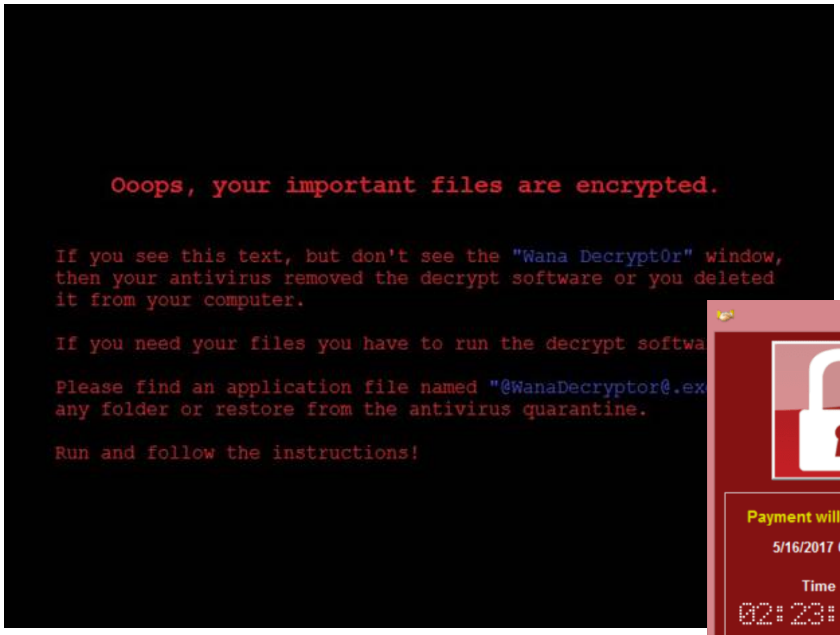
Vector: It uses ETERNALBLUE (SMBv1) MS17-010 to propagate. Windows XP and Windows 2003 do have the MS17-010 patch. There is code to 'rm' (delete) files in the virus. Seems to reset if the virus crashes

Financial impact: Estimated at hundreds of millions up to $4 billion. Between $300 and $600 per infected machine

Example infections: NHS (UK), Telefonica (Spain), FedEx (US), University of Waterloo (CA), Russia interior ministry and Megafon (Russia), Сбера bank (Russia), Shaheen Airlines (India), Neustadt Station (Germany), University of Milan (Italy), among others

Spread: Over 200,000 systems in 150 countries by morning of May 15, 2017

What you see…



Where do the encryption keys get sent?

The AES keys are generated with a CSPRNG, CryptGenRandom

The following C2 servers have been identified (all TOR hidden servers):

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52ma.onion
- sqjolphimrr7jqw6.onion

Where does the money go?

Three addresses for Bitcoin wallets are hard-coded into the Wannacry malware

- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Paying ransom is not recommended by the FBI:

- There is no guarantee that data will be returned
- Small amounts for ransoms add up with large-scale infections
- Proceeds are used to support additional criminal activity
- Consider paying ransom only as a last resort

WannaCry – It’s not all bad news (or is it?)

- It seems to only be ransomware – Could have been used for exfiltration/theft but does not appear to have been
- It wasn’t targeted on us
- It actually wasn’t great malware – kill-switch, little obfuscation
- Microsoft came to the rescue! XP patches?! 2003 patches?!
- Wasn’t really geared for monetization
- Bloggers, researchers also came to the rescue
- Backup, patching and upgrades will now improve

But what about next time?

Preparing for ransomware attacks

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 15, 2016

Alert Number
I-091516-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

RANSOMWARE VICTIMS URGED TO REPORT INFECTIONS TO FEDERAL LAW ENFORCEMENT

The FBI urges victims to report ransomware incidents to federal law

Prevention and remediation steps:

- Establish and maintain rigorous patching practice
- Implement backup and recovery strategy based on system recovery time objective (RTO) and recovery point objective (RPO)
- Ensure that backups are not connected and susceptible to infection
- Disconnect device from network to prevent further infection
- Restore system and patch in protected environment prior to reconnecting to prevent reinfection
- Contact FBI field office to report event and provide evidence, if available
- The FBI recommends not paying the ransom as a general rule

KPMG

Landscape focus: Cyber surveys

KPMG's Healthcare Cybersecurity Survey

- 80% have reported a breach in the past 12 months
- 53% of Providers and 66% of Payers consider themselves ready for a cyber attack
- Only 13% say they are tracking attacks every day on their infrastructures.
- 27% do not have a dedicated security leader and 45% do not have any Security Operations Center (SOC) capability
- Our conclusion: Most of the industry is able to identify and react to yesterday's threats, not the new normal

233 Healthcare Executives (Payers and Providers) surveyed. 44% were Not-for-profit organizations. All had revenue over $500 million, 70% had revenue over $1 Billion.

The top seven causes of information security breaches:

1. **Naive end users**
   Lack of security awareness training and accountability
2. **Misconfigurations or human errors**
3. **Malicious software**
   viruses, worms and trojans
4. **Lost or stolen computers**
   including mobile devices
5. **Disgruntled Employees and Contractors**
6. **Came into focus of mass media**
7. **Insufficient funding**
   of IT and Information Security

KPMG's Healthcare Cybersecurity Survey
(continued)

- Of the top seven reported causes of a security breach, five are people or process based.
- According to a recent HIMSS security survey:

"The greatest security threat to patient data is that it will be compromised by an organization's staff. Eighty (80) percent of respondents noted that they were concerned that human-related factors would put data at risk. Furthermore, respondents were most likely to indicate the greatest motivator leading to the compromise of data is for workforce members to snoop on co-workers, friends and neighbors patient information".

The top seven causes of information security breaches:

1. **Naive end users**
   Lack of security awareness training and accountability
2. **Misconfigurations or human errors**
3. **Malicious software**
   viruses, worms and trojans
4. **Lost or stolen computers**
   including mobile devices
5. **Disgruntled Employees and Contractors**
6. **Came into focus of mass media**
7. **Insufficient funding**
   of IT and Information Security

KPMG's 2017 Healthcare Cybersecurity Survey

Among known attacks within the past year, which vectors compromised your environment?

- External attacker	72%
- Phishing-introduced malware	55%
- Third-party undetected vulnerability	43%
- Internal bad actor	34%
- Undetected vulnerability within a system Configuration	31%

Bad actors are motivated by ransoms and revenge

How much goes undetected?

KPMG's 2017 Healthcare Cybersecurity Survey

What are the most important information security concerns you have at your organization?

- Malware	72%
- HIPAA violations/compromise of patient privacy	55%
- Internal vulnerabilities (employee theft/negligence)	47%
- Aging IT hardware	40%
- Shortage of qualified IT staff	38%
- Out-of-date security software	35%
- Medical device security	35%

32% of healthcare firms have had ransomware introduced into their environment

47% of healthcare firms have had a HIPAA-related security violation or breach in the past two years

KPMG's 2017 Healthcare Cybersecurity Survey

Where has your organization made investments in information security?

- Stronger policies/controls	82%
- Greater technology investments	79%
- Governance (setting a tone at the top)	49%
- Managed services	47%
- Consulting	41%
- Hardware	28%
- Staff	24%

KPMG's 2017 Healthcare Cybersecurity Survey

In the event of a data breach at your healthcare organization, which of these concerns would be the most important?

- Regulatory enforcement	30%
- Litigation	28%
- Reputation	25%
- Financial loss	17%

KPMG's 2017 Healthcare Cybersecurity Survey

If your organization was infected with ransomware, what was your organization's initial response to handle the infection?

- Pay the ransom	41%
- Use a forensic team to fix the problem	25%
- Work-arounds (redundant systems)	16%
- Work with authorities	19%

80% of organizations' executive leadership (C-suite) has discussed the possibility that their systems may be attacked with ransomware in the future

KPMG's 2017 Healthcare Cybersecurity Survey

KPMG analysis:

- Dangerous period with regard to healthcare cyber risks
- Focus has been on electronic health records since ARRA
- IT management and cybersecurity maturity lag behind healthcare application and data growth
- Bad actors continuously improve their own craft
- Increased likelihood that the number and severity of assaults and breaches increase
- Continued myopic focus on tools without realizing benefits

Verizon Cybersecurity Survey

The 2017 Verizon Data Breach Investigations Report found these Top 3 Healthcare-related attacks (representing 81% of Healthcare breaches):

Insider and privilege misuse

Errors

Physical theft/loss

KPMG’s viewpoint -
What can we do about it?

The new normal in Healthcare

Healthcare organizations are facing increased security threats by:

- The **evolving threat landscape**, where cyber attacks today are more sophisticated and well-funded given the increased value of the compromised data on the black market
- The **adoption of digital patient records** and the automation of clinical systems
- The use of **antiquated EMR and clinical applications** that are not designed to securely operate in today's networked environment and software vendors that push that problem to the provider
- The **ease of distributing ePHI** both internally (laptops, mobile devices, thumb drives) and externally (third parties, cloud services)
- The **heterogeneous nature** of networked systems and applications (i.e., network-enabled respirator pumps on the same network as registration systems that can browse the Internet)

The new normal in Healthcare - Themes

New threat model

Compliance does not equal cyber maturity

Security threats are not confined to your own organization

Increase cyber Investments – In the right order

The new normal in Healthcare - Trends

Current Trends:

Extortion-driven attacks and **ransomware** attempts will increase and will become more threatening (moving in to backups, more theft, etc.)

EMR interoperability will provide larger attack surface, requiring new thinking and solutions, such as **blockchain**, patient ownership of data, etc.

Widespread use of **medical devices** and **IoT** (internet of things) brings a parallel increase in risk

Insider threat will be brought into greater focus as technology improves, allowing visibility into credential abuse

Organizations will focus much more on risks posed by **third-party vendors** and **suppliers**

The new normal in Healthcare - Trends

Trends on the <u>mid term</u> Horizon:

- Resurgence in strategic web compromise (watering holes, malvertising) for targeted attacks
- Increased cloud security requirements
- Mobile device security
- Telemedicine vectors
- Increased concern around business email compromise

The new normal in Healthcare - Trends

Trends on the long term horizon:

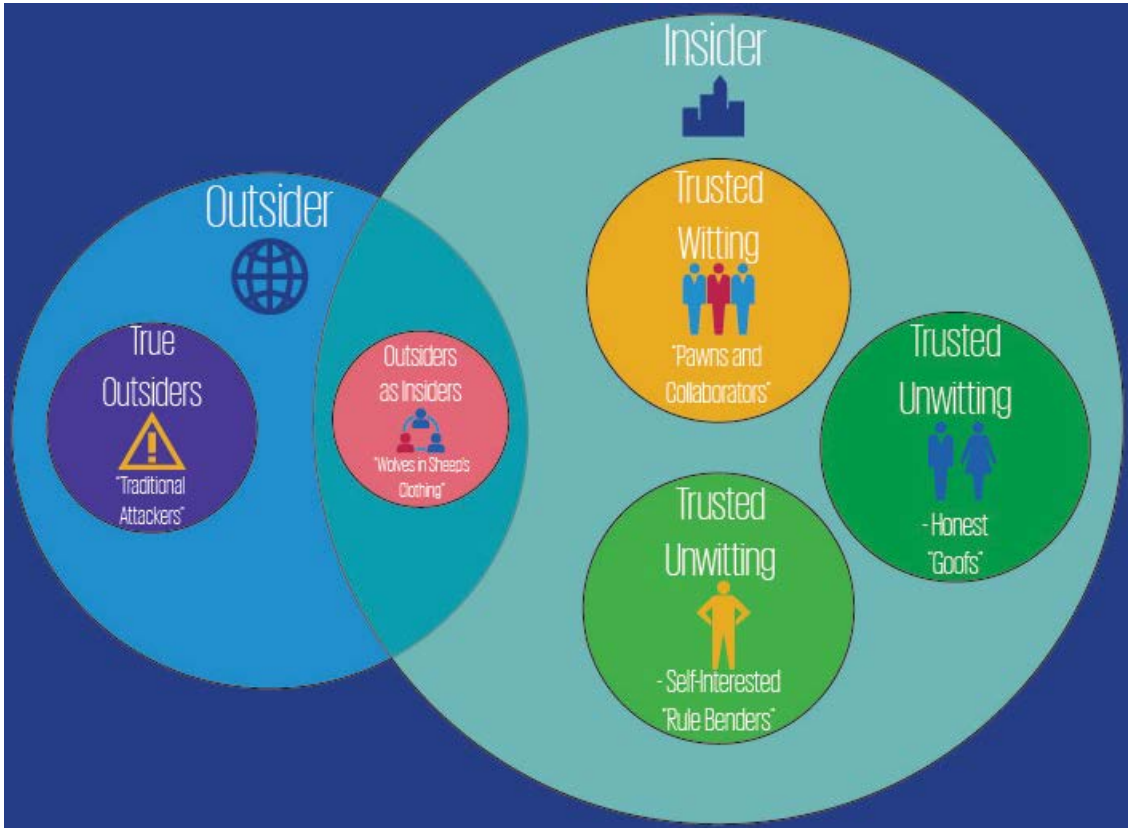
- Medical device interruption – Not current threat but interest building
- Medical research – Move from just theft to include sabotage
- DNA data – Not currently targeted yet but possibly will be in a few years
- OT medical devices that are not air-gapped – Currently more intention than capability
- Genome editing/corruption

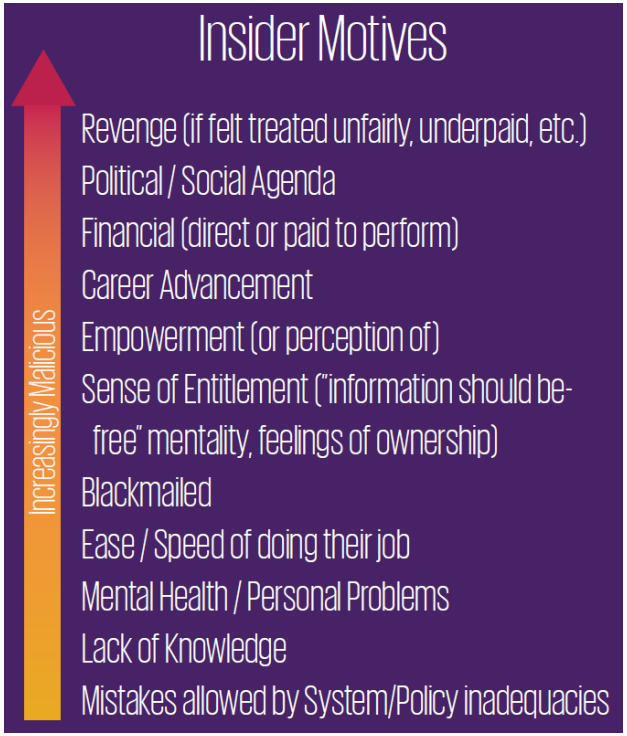
KPMG

Viewpoint focus: The insider threat

The insider threat

There are many types of insider threats with motives ranging from unintentional to malicious





Insider threat trends

There are many trends driving growth of insider threats

Changes in Employees	Changes in Work Environment	Changes in Technology	Changes in the World
Dynamic nature of career paths decreases employee loyalty	Obsolescence of traditional network defense	Increased dependence on interconnected technology	The rise of social media
Views of knowledge being "open-source"	Network access anywhere and BYOD	Increased capabilities in machine learning	Volatile and delicate world stage
High Gen Y turnover rates	Increased inter-dependence on 3rd party partners		Rising distrust for authority
	Emergence of the cloud		Rise in dark web

The essence of insider threat is different

Though the basic elements of the NIST-CSF are still relevant to addressing Insider Threats, there are many differences. Standard methods of prevention, detection, and response are ineffective at mitigating potential Insider Threat Incidents :

	Traditional "External" Perspective	Insider Threat "Internal" Perspective
Protect	• Firewalls • IPS (intrusion prevention system) • Sandboxes	• Cultural implications • Insider threat awareness/training • Third-party management • Full employee life cycle perspective • Workplace violence/employee assistance Programs
Detect	• Focus on perimeter • Dependence on malware signatures • Malicious IP blacklisting • IDS (intrusion detection system)	• Monitoring behavior with machine learning/ anomaly detection/pattern recognition • Risk score and "faint signal" build up • Predictive analysis • Whistle-blower (nontechnical) programs • Wider data sources (including unstructured, physical, HR, etc.)
Respond	• Incident Response Playbooks • Investigation Tools • System Containment/Recovery	• Forensic case management more complex (considering legal implications, etc.) • Fraud investigation/remediation • Information obfuscation requirements • Packet/video replay
Governance	• Board engagement	• Board engagement • Cross-organization coordination • Privacy laws/compliance • Risk management to include employees

KPMG

Viewpoint focus: Penetration testing

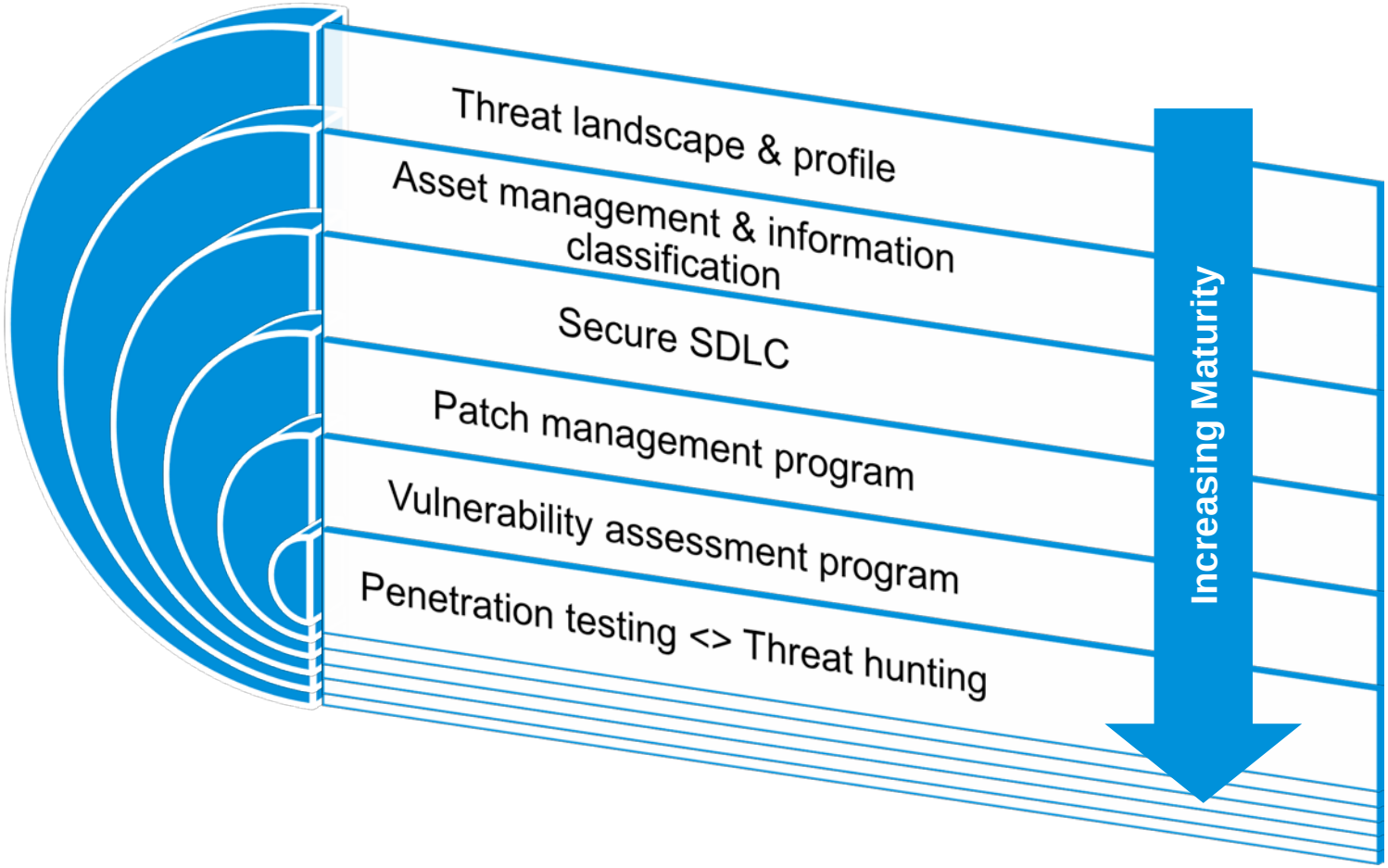
Penetration testing +/-

The venerable penetration test, while still a mainstay in cybersecurity has both pluses and minuses in the current landscape:

- **Proactive –** Doesn't wait to be breached
- **Target based –** Real-world and specific
- **Historic success –** Been done for a long time
- **Client-specific –** Can find issues unique to the specific entity

- **Only deals with the known –** *The quote that it "uses same thinking as attackers" should add the phrase "…did yesterday"*
- **Only as good as the White Hat –** *What if Black Hat is better?*
- **Target based –** *Only goes after one/few vectors*
- **Not current –** Often not regular/current

Penetration testing in the maturity stack



Trends in penetration testing

Moving from manual to **automated**

Commoditization of penetration testing

Increasingly **collaborative**. Integrated multi-user

Beginning to see **crowdsourcing** – Many perspectives and players

Increase in **vulnerability scanner capability**

Increasing perspective on **threat hunting**

Emphasis on layer 7 (application) Network mostly locked down

KPMG’s viewpoint -
What can we do about it?

Summing it up…

Building a cyber program with the business

Organizations universally agree: Cyber resource and investment allocations must be balanced between traditional reactive security measures, more proactive business enablement, and advanced sustainability objectives.

Cyber defense	Business enablement	Resilience
Cyber defense includes actions and infrastructure intended to defend the perimeter.	Business Enablement involves cyber teams working collaboratively with business owners.	Resilience represents an organizational commitment to cyber maturity.

Building a reliable structure for the business

The building blocks to technology services and cybersecurity

- Target operating model
- Training & awareness
- Identify & access management
- Asset management & data asset classification
- Secure development & delivery
- Incident response
- Vulnerability management
- Security operations & monitoring
- Network security architecture
- Privileged access management
- Governance risk & compliance

Data center consolidation | **New technology & capabilities** | **Integration of acquisitions**

email | Internal apps | External apps (cloud) & services

Technology services | Core network | Core OS | (building the foundation to support the business)

Cyber maturity lenses

Legal and compliance

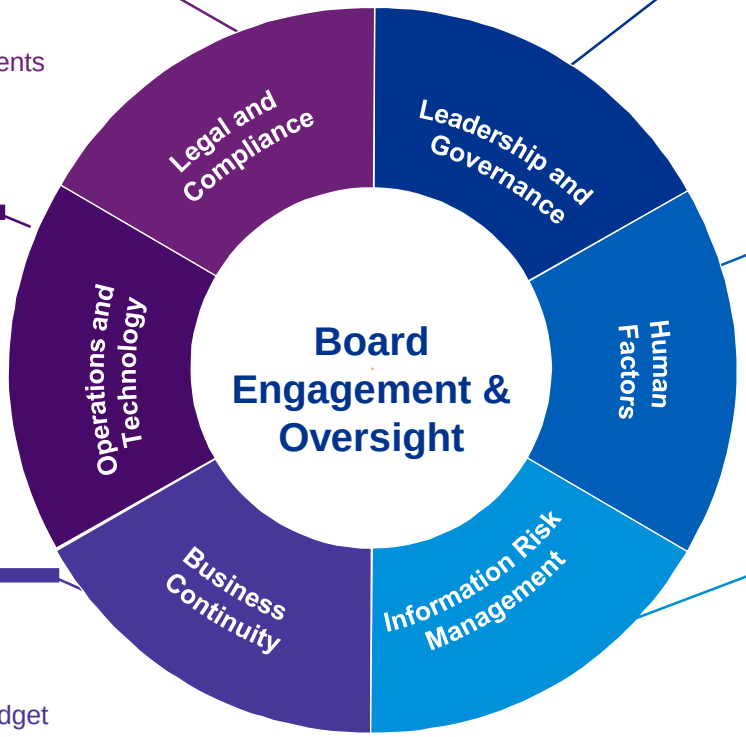
- Inventory of compliance requirements
- Compliance program components
- Role of the audit committee
- Litigation inventory
- Cyber insurance

Operations and technology

- Threat and vulnerability management
- Logical security controls
- Physical security controls
- Security monitoring
- Incident response
- Integration with IT service management

Business continuity and crisis management

- Ability to manage cyber event
- Financial ramifications and budget
- Resources required and training
- Detailed plans
- Communications
- Testing



Leadership and governance

- Board involvement
- Third party supplier relationships
- Identification of critical data
- Ownership and governance for data protection
- Project management

Human factors

- Training and awareness
- Culture
- Personnel security measures
- Talent management
- Organizational roles and responsibilities

Information risk management

- Risk management approach and policies
- Risk tolerance identification
- Risk assessment and measures
- Change management
- Information sharing
- Third party accreditation
- Information communication architecture

Call to action

New threat model

- Organizations have to align their security programs to the new threat model
- Full attention should be paid to the insider threat as well as the external attacker

Compliance does not equal cyber maturity

- Organizations need to assess cyber maturity against a more rigorous standard, not just regulatory compliance
- Integrate cybersecurity with compliance to drive organization wide initiatives
- Stronger reporting structure for the TOM (target operating model) and responsibility to not just the CIO but also to Compliance and the board

Security threats are not confined to your own organization

- Organizations have to improve their communications both internally and externally
- Integrated cybersecurity technologies, with strong reporting and monitoring capabilities

Increase cyber Investments – In the right order

- We need to invest in cybersecurity across the paradigm of people, process and technology
- Only invest in technology with a measurable plan!
- Attend to the basics first, build the right foundation before trying to advance

Thank you

Michael Thompson
Director – Cyber Defense
MDThompson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia