Hacking the C-Suite:
86% of CIOs Say You're Not Doing Enough

Anil Markose, Principal and Cyber Threat Management Leader, Ernst & Young

2017 NMHC Spring Board of Directors Meeting
May 16-18, 2017
AGENDA

• Understanding the current state of cybersecurity
• How does this affect you
• Best practices and considerations
THE PERFECT STORM....

35

Days for a new technology to reach a critical mass of 50m users

Mobile
Big Data
Cloud Computing
Social
Internet of Everything

50bn

Internet connected “things” by 2020** including sensors, RFID chips etc

86% of organizations believe there’s a shortage of skilled cybersecurity professionals. By the year 2020, the deficit of cybersecurity professionals to job opportunities is expected to reach over 1.5 million.*


1%

According to Cisco, only 1 percent of devices that could be connected in the world actually is

240+ Days

Average amount of time an attacker is on a corporate environment before detection
There are two types of companies: those that have been breached, and those that don’t know it yet.
• 87% of board members and C-level executives have said they lack confidence in their organization’s level of cybersecurity

• 73% are concerned about poor user awareness and behavior around mobile devices

• 57% of responders have had a recent significant cybersecurity incident

• 42% do not have an agreed communications strategy or plan in place in the event of a significant attack

• 86% say their cybersecurity function does not fully meet their organization’s needs
HOW DOES THIS AFFECT YOU

Know where sensitive data flows
BEING ATTACKED IS UNAVOIDABLE – BE PREPARED

1. Do you know what you have that others may want?
2. Do you know how your business plans could make these assets more vulnerable?
3. Do you understand how these assets could be accessed or disrupted?
4. Would you know if you were being attacked and if the assets have been compromised?
5. Do you have a plan to react to an attack and minimize the harm caused?

Valued assets

- Intellectual property
- People information
- Financial information
- Business information

Would you know if an attacker was able to gain access to your most valuable information?
Take an unorthodox approach:

- Switch from a “fail safe” mindset to a “safe to fail” mindset
- Shift from protection to sacrifice
Anil Markose
Principal and Cyber Threat Management Leader
Ernst & Young LLP
(212 773 1770)
Anil.Markose@ey.com