Resilience
The cyber-shock absorber businesses need
Session objectives

- Fast facts
- Strengthening the digital society against cyber shocks
  - To compete in the emerging digital world, companies should protect themselves from cyber risks, and become more resilient to cyber shocks
- Protect.me
  - How Consumers See Cybersecurity and Privacy Risks and What to Do About It
- Emerging Technologies
Sources

• The Global State of Information Security® Survey 2018, a worldwide study by PwC, CIO and CSO, was conducted online from April 24, 2017 to May 26, 2017.
  - PwC’s 20th year conducting the online survey, 15th with CIO and CSO
  - Responses from more than 9,500 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices
• Consumer Intelligence Series: Protect.me
  - During August and September 2017, PwC surveyed a nationally representative sample of 2,000 Americans over the age of 18 via an online survey and video interviews.
• PwC’s 20th CEO Survey
  - 1,379 CEOs interviewed in 79 countries
Fast facts
Organizations continue to move to the cloud

50% of all IT services, on average, are delivered via cloud service providers
Current employees are the number one source of incidents

19% of incidents are attributed to organized crime but current employees remain the number one source of security incidents.
Third-party partners continue to create exposure

62% of incidents are attributed to third-party business partners. Incidents attributed to insiders have declined while those ascribed to outsiders inched up.
For consumers, cyberattacks are personal

45% of respondents believe their email or social media accounts will get hacked in the next year—more than those who assume they’ll have a flight cancelled (36%) or get in a car accident (20%).
Consumer trust is fading

87% of consumers say they will take their business elsewhere if they don’t trust a company is handling their data responsibly.
Strengthening the digital society against cyber shocks
What is cybersecurity?

- Integrity
- Confidentiality
- Availability
What is data privacy?
Why cybersecurity is an imperative

9,576 Number of phishing attacks reported in 2016¹

64% Percentage of Americans that have had their data affected by a breach²

63% Percentage of breaches last year that involved weak, stolen, or default passwords¹

¹ Verizon 2016 Breach Investigations Report
² 2017 Pew Research Center
# Cybersecurity
The threat landscape

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Motives</th>
<th>Targets</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nation State</strong></td>
<td>• Economic, political, and/or military advantage</td>
<td>• Trade secrets</td>
<td>• Loss of competitive advantage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sensitive business information</td>
<td>• Disruption to critical infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Emerging technologies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical infrastructure</td>
<td></td>
</tr>
<tr>
<td><strong>Terrorists</strong></td>
<td>• Immediate financial gain</td>
<td>• Critical Infrastructure</td>
<td>• Disruption to critical infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Influence political and/or social change</td>
<td>• Anything of value</td>
<td>• Policy/social change</td>
</tr>
<tr>
<td></td>
<td>• Identify and attract supporters</td>
<td>• Ideological supporters</td>
<td>• New supporters</td>
</tr>
<tr>
<td><strong>Organized Crime and Criminals</strong></td>
<td>• Immediate financial gain</td>
<td>• Financial/Payment Systems</td>
<td>• Costly regulatory inquiries and penalties</td>
</tr>
<tr>
<td></td>
<td>• Collect information for future financial gains</td>
<td>• Personally Identifiable Information</td>
<td>• Consumer and shareholder lawsuits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Payment Card Information</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protected Health Information</td>
<td></td>
</tr>
<tr>
<td><strong>Hacktivists</strong></td>
<td>• Influence political and/or social change</td>
<td>• Corporate secrets</td>
<td>• Disruption of business activities</td>
</tr>
<tr>
<td></td>
<td>• Pressure business to change their practices</td>
<td>• Sensitive business information</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Information related to key executives, employees, customers &amp; business partners</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td><strong>Insiders</strong></td>
<td>• Personal advantage, monetary gain</td>
<td>• Sales, deals, market strategies</td>
<td>• Trade secret disclosure</td>
</tr>
<tr>
<td></td>
<td>• Professional revenge</td>
<td>• Corporate secrets, IP, R&amp;D</td>
<td>• Operational disruption</td>
</tr>
<tr>
<td></td>
<td>• Patriotism</td>
<td>• Business operations</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Personnel information</td>
<td>• National security impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recent breaches

Equifax

143M Records

Instances of the vulnerability that allowed a hacker to upload a backdoor into Equifax exist today

"WannaCry"

Microsoft releases security bulletin and patch to fix identified vulnerability

Unpatched server is compromised

Equifax detects breach and disables server

WannaCry

$869M Losses

The WannaCry ransomware impacted more than 203,000 in over 150 countries

"WannaCry" infects more than 230,000 computers in over 150 countries

Shadow Brokers leak NSA developed exploit, Eternal Blue, out for use as "WannaCry" ransomware

May

June

July

August
WannaCry Ransomware – A new breed of attack

**Lesson’s learned:**

- Threat intelligence would have allowed an early warning once the Shadow Brokers (NSA) leak occurred on Wikileaks; IOCs could have been created to identify this type of attack and contain it
- Timely patch management would have prevented the attack – patch was released on March 14 - 2017
- Preventing risky services (SMB v1) from running on workstations and/or allowing workstations to be accessed by hostile computers on the internet (hardening, firewalls, and network segmentation)

**Impact**

**Delayed health treatment**
- The UK’s NHS said 16 of its organizations were impacted and patients were turned away.

**Car Maker Closes Plant**
- One of Renault’s biggest factories in France remained closed on Monday as a “preventative” measure in the wake of the global cyberattack. Renault had to temporarily lay off 3,500 staff at their Douai factory in France, giving them a holiday on Monday while they try and limit damage to the factory’s computers.
How Ransomware works

Ransomware is Evolving by the Hour: Unlike traditional malware, which is frequently reused across a wide range of targets, ransomware strains are typically mutated for each new victim. Traditional anti-virus solutions that rely on blacklists are typically ineffective in preventing ransomware.

A Common Path to Encryption: Actions executed by ransomware across different families all followed similar subsequent processes. Typically, the malware first attempted to communicate back to an attacker-managed key server, which held the unique public key used to encrypt files on the machine. Second, the ransomware began to scan the infected machines to locate specific files types. Third, upon locating the files, the ransomware began the encryption process.

Ransom Payment Method of Choice: To receive the key needed to decrypt the impacted files, users were required to submit payment to the attackers. Payment was typically demanded in Bitcoin, and for Bitcoin novices, some attackers went so far as to set up “help desks” to help victims purchase Bitcoin and complete the funds transfer.

Ransomware Seeks Admin Rights: In the majority of cases, ransomware attempted to gain local administrator rights once activated. But interestingly, only a fraction of the files failed if these rights could not be attained. This shows that even though the removal of local administrator rights from standard users is a best practice and certainly could have prevented ransomware, this measure must be layered with application control to reliably protect against file encryption.

A Common Denominator: A highly effective way to mitigate the risk of ransomware attacks is to prevent unknown applications, including unknown ransomware, from gaining the read, write and edit permissions needed to encrypt files. A combined approach of removing local admin rights and application control, including greylisting, which restricts read, write and modify permissions from unknown applications was extremely effective in preventing ransomware from encrypting files.

FTC Commissioner Edith Ramirez presented at a workshop and noted that the average ransomware ransom demands roughly $570 at time of infection, though the price tends to increase when victims delay payment. Source: http://fedscoop.com/ftc-chief-ransomware-malware-september-2016
CIA’s hacking tool kit is leaked by Wiki Leaks

**Threat overview**

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Likely an disgruntled insider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Motive</td>
<td>Expose or embarrass the CIA</td>
</tr>
<tr>
<td>Threat Vector</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

**Target(s)**

CIA’s Computer Operations Group

**Impact**

**IoT Compromise**
- Weeping Angel – Smart TV implant kit that allows a Smart TV to be turned into a listening device

**Networking devices**
- Significant vulnerabilities in Netgear, Cisco, Huawei, HP networking equipment

**Mobile devices**
- A variety of unpublished iOS and Android exploits

**Takeaway**: New tools and exploits will be available to hackers; Even nation states will use “retail” hacking tools if they can get in with more simple means
“Old” Friends
In 2017, global respondents detected 30% fewer security incidents*

Respondents across most industries have seen double digit decreases in the number of detected security incidents, including Entertainment & Media and Telecommunications, which both saw the number of incidents decrease by over 50%. Only 4 of 12 sectors reported increases in security incidents.

**Average number of security incidents in past 12 months**

* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: “What is the number of security incidents detected in the past 12 months?”
With fewer security incidents detected, average financial losses dropped 16%

Most sectors reported decreases in financial losses including Telecom which decreased by 33% and Retail and Consumer which decreased by 24%. Only 4 of 12 sectors reported increases in financial losses as a result of security incidents.

Average estimated total financial losses by industry

- Entertainment & Media: $3.5M
- Financial Services: $2.7M
- Retail & Consumer: $2.5M
- Technology: $2.1M
- Telecom: $3.3M

Decrease in average financial losses among large organizations

Question 22A: Estimated total financial losses as a result of all security incidents
Email compromise continues to be the top business impact of incidents

Recently, cyber extortion, where a cyber criminal threatens to publically embarrass or threaten a company to secure large sums of money, has become an increasingly common approach taken by threat actors as evidenced in the case of film/television production and distribution companies and a number of hospitals. Thus, financial losses as a business impact of an incident may begin to climb.

Business impacts of security incidents

- Theft of "hard" intellectual property: 17%
- Brand/reputation compromised: 17%
- Financial losses: 22%
- Theft of "soft" intellectual property: 23%
- Business email compromise: 24%

Cite mobile device exploitation as the cause of security incidents, overtaking phishing attacks as the top threat vector.

Question 22: “How was your organization impacted by the security incidents?”
Question 19: “How did the security incident(s) occur?”
**Current employees are still the number one source of security incidents**

Incidents attributed to outsiders, such as hackers and competitors, declined while those attributed to insiders such as third parties and employees stayed about the same or inched up.

*Estimated likely source of incidents*

- 20% Current third parties*
- 23% Competitors
- 26% Unknown hacker
- 28% Former employees
- 29% Current employees

*Current third parties include suppliers, consultants and contractors

Question 21: “Estimated likely source of incidents” (Not all factors shown.)

19% Of incidents are attributed to organized crime
The impact of data-related security incidents is shifting from compromising data confidentiality to data integrity

Cyberattacks that manipulate or destroy data can undermine trusted systems without the owner’s knowledge and have the potential to damage critical infrastructure.

Data impacts of security incidents

- Customer records compromised
- Employee records compromised
- Loss or damage of internal records

Question 22: “How was your organization impacted by the security incidents?”

Report loss or damage of internal records as a result of a security incident (+3% YoY)
Organizations continue to move critical functions to the cloud including IT, operations, finance and marketing/sales

An average of 50% of IT services are delivered using the cloud. The same cloud vendors are often shared by multiple large corporations, increasing the chance of systemic failures which may impact these companies, their consumers and society in currently unforeseen ways.

Business functions run in a cloud environment

Question Q15_2017: “What business function areas does your organization run in a cloud environment?”

Question Q16_2017: “Currently, what percentage of your organization’s IT services is delivered via cloud service providers?”
This year, organizations are prioritizing spending on broad strategies to strengthen their digital ecosystems

Security priorities in 2017 emphasize internal collaboration and new security safeguards for evolving business models. Biometrics and advanced authentication has notably increased as an investment priority compared to 2016 (+3% YoY).

Information security spending priorities for 2017

- Digital enterprise architecture: 43%
- New security needs related to evolving business models: 45%
- Security for the Internet of Things: 45%
- Biometrics & advanced authentication: 46%
- Improved collaboration among business, digital & IT: 49%

59% of respondents say digital transformation has increased information security spending.

Question 10a_2017: “What types of security safeguards does your organization plan to invest in over the next 12 months?”

Question 10_2017: “What impact has digitization of the business ecosystem had on your organization’s security spending?”
The essential eight technologies

- Internet of Things
- Augmented reality
- Virtual reality
- 2020 outlook
- Drones
- Robots
- 3D printing
- Blockchain
- Artificial intelligence
Anticipated results of a successful cyberattack against automation and/or robotics systems

- **40%** Disruption of operations/manufacturing
- **39%** Loss or compromise of sensitive data
- **32%** Negative impact to quality of products produced
- **29%** Damage to physical property
- **22%** Harm to human life

Cloud and IoT adoption will increase the attack surface, and cyber attacks have continued to impact corporations

To address these issues, a recent US National Security Telecommunications Advisory Committee report calls for research and action in areas such as machine learning and increased technology interoperability, the former of which already has traction among corporations.

Reported benefits of a Big Data-driven security capability

- Improved ability to quickly identify and respond to security incidents: 41%
- Better visibility into anomalous network activity: 41%
- Improved understanding of user behavior: 41%
- Improved understanding of internal security threats: 49%
- Improved understanding of external security threats: 61%

Use Big Data analytics to model for and identify information security incidents (+4% YoY)

Question 13a_2016 What are the most significant benefits of a Big Data-driven security capability?
Question 18_2015 Does your organization employ Big Data analytics to model for and identify information security incidents?
## IoT’s design presents risks

<table>
<thead>
<tr>
<th>IoT Trait</th>
<th>Related Security Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Purpose Design</td>
<td>Not designed for security</td>
</tr>
<tr>
<td>Data Intensive</td>
<td>Large quantities of data complicate detection</td>
</tr>
<tr>
<td>Process personally sensitive information</td>
<td>Contains valuable data of interest to attackers</td>
</tr>
<tr>
<td>Works with critical assets</td>
<td>Vector of attack into critical assets</td>
</tr>
<tr>
<td>Controls physical devices</td>
<td>Security failures can lead to injury or death</td>
</tr>
<tr>
<td>Utilize complex and proprietary technologies</td>
<td>Difficult to design security solutions for</td>
</tr>
</tbody>
</table>

### Fast Facts

- **only 39%** of companies have a security strategy around IoT.
- The FDA and other government agencies are starting to issue guidance around IoT.
- IoT security revenue is expected to quadruple from $6.9b in 2015 to $28.9b in 2020 over the next 4 years.
As Internet of Things becomes more ubiquitous, organizations are investing in revamping their security policies

Consumers are demanding products with an emphasis on cybersecurity and privacy. This is reflected in key IoT investment areas including policies and technologies to protect consumer privacy, as well as data governance policies.

Policies, technologies & people skills being implemented for the Internet of Things

- Policies & technologies to safeguard against consumer privacy violations: 31%
- Employee training on IoT security practices: 32%
- Assess device & system interconnectivity & vulnerability across the business ecosystem: 34%
- New data collection, retention & destruction policies: 34%
- Uniform cybersecurity standards & policies for IoT devices & systems: 36%

67% of organizations have an IoT security strategy in place or are currently implementing one (+5% YoY)

Question 25_2017: “What policies, technologies and people skills does your organization plan to implement over the next 12 months to address the cybersecurity and privacy risks associated with the Internet of Things (IoT)?”

Question 17_2015 Does your organization have a security strategy for the convergence of information, operational, and consumer technologies (also known as the Internet of Things)?
**Key findings**

It’s critical that companies understand and respond appropriately to their customers’ cybersecurity concerns.

To earn consumers’ trust, you must vigorously protect customers’ data while respecting individual privacy as you look for ways to monetize that data.
Key findings (continued)

69% Of consumers believe companies are vulnerable or extremely vulnerable to hacks and cyberattacks.

25% Of respondents believe most companies handle their sensitive personal consumer data responsibly.

10% Of consumers feel they have complete control over their personal information.

72% Of consumers believe businesses, not the government, are better equipped to protect them.
For consumers, cyberattacks are personal

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>My email or social media accounts get hacked</td>
<td>45%</td>
</tr>
<tr>
<td>My flight is cancelled</td>
<td>36%</td>
</tr>
<tr>
<td>I get a new job</td>
<td>35%</td>
</tr>
<tr>
<td>I have to go to the ER</td>
<td>31%</td>
</tr>
<tr>
<td>I’m a victim of credit card fraud</td>
<td>29%</td>
</tr>
<tr>
<td>I win money in the lottery</td>
<td>25%</td>
</tr>
<tr>
<td>I get food poisoning</td>
<td>24%</td>
</tr>
<tr>
<td>My employer gets hacked/is subject to a cyberattack</td>
<td>21%</td>
</tr>
<tr>
<td>I’m involved in a car accident</td>
<td>20%</td>
</tr>
<tr>
<td>My identity gets stolen</td>
<td>18%</td>
</tr>
<tr>
<td>My insurance company refuses to pay a claim</td>
<td>17%</td>
</tr>
<tr>
<td>My home gets burglarized</td>
<td>8%</td>
</tr>
</tbody>
</table>

Q: Which three of the following scenarios do you think is most likely to occur to you in the next year?
Source: PwC US Protect.me Survey, 2017
Consumer trust is fading

The stark reality is consumers trust companies less today than in the past. Only 12% of consumers said they trust companies more than they did a year ago, while 17% trust companies more today than a decade ago.
Consumer trust is fading

- **25%** Of respondents believe most companies handle their sensitive personal data responsibly.
- **12%** Of consumers said they trust companies more than they did a year ago.
- **88%** Of consumers agree the extent of their willingness to share personal information is predicated on how much they trust a given company.
- **15%** Think companies will use that data to improve their lives.
- **17%** Trust companies more today than a decade ago.
- **87%** Of consumers say they will take their business elsewhere if they don’t trust a company is handling their data responsibly.
Who’s on the hook?

Consumers want both companies and the government involved, but say companies bear a larger share of the responsibility.

Consumers also expect more from regulators.
Who’s on the hook?

- **92%** agree companies must be proactive about data protection.
- **82%** say the government should regulate companies’ use of data.
- **72%** believe companies are better equipped than the government to protect their data.
- **70%** say government is ineffective in ensuring fair use of their data.
- **60%** say the responsibility of protecting data rests with the company collecting the data.
- **80%** agree that government regulation of new technologies is crucial for consumer protection.

Unlike the European Union’s approach to data privacy regulation—known as the General Data Protection Regulation (GDPR)—most US data privacy laws vary by sector, data type, or from state to state.
The path to trust
Giving customers control and providing transparency

Consumers want control over their data, but they don’t feel like they have it.

Consumers believe companies should have cybersecurity and privacy policies in place to protect their sensitive information.

If companies don’t adequately protect consumer data, they risk consequences from regulators and consumer backlash.
The path to trust (continued)
Giving customers control and providing transparency

85% of customers will not do business with a company if they have concerns about its security practices.

Q: How much do you agree or disagree with the following statements?
Source: PwC US Protect.me Survey, 2017

- 92% Say they should be able to control the information available about them on the internet
- 91% Say companies should notify consumers about all data breaches
- 88% Say the amount of data they share with a company depends on how much they trust it
- 87% Want the ability to remove their personal data from the internet if it hurts their reputation
- 85% Say cybersecurity and privacy risks are among the biggest risks facing society
- 71% Find companies’ privacy rules difficult to understand
What types of businesses do consumers trust most?

69% of CEOs said it is becoming much more difficult for businesses to earn and keep trust in a digital world.

*PwC’s 20th Global CEO Survey*
Q: Which of the following industries or company types are the most trustworthy? Choose top five.
Source: PwC US Protect.me Survey, 2017
Consumer perceptions of industries’ trust and cyber risks

Consumer Intelligence Series: Protect.me

Q: Which of the following industries or company types are the most trustworthy?
Source: PwC US Protect.me Survey, 2017

More trusted industries include:
- Healthcare Providers
- Hospitals
- Utilities
- Nonprofits

Less trusted industries include:
- Social Media
- Online Retailers
- Media & Entertainment
- Startups
- Telecom
- Air Lines
- Advertising

Considered more risky industries include:
- Professional Services
- Pharma
- Energy/Oil/Gas
- Food & Beverage
- Aerospace
- Automotive
- Sports
- Construction/Real Estate
- Agriculture
- Manufacturing
- News
- Hotel

Considered less risky industries include:
- Government
- Information Technology
- Banks
- Insurance Companies

Source: PwC US Protect.me Survey, 2017
After a data breach, can companies earn back consumer trust?
How companies can regain trust after a data breach?

- **27%** Compensate victims of the breach
- **22%** Tell customers what happened and how it is being resolved
- **20%** Provide proof that the right systems are in place
- **19%** Offer complementary security services to ensure customers’ data is safe
- **5%** Reaffirm its privacy policy in a clear message
- **4%** Other
- **3%** Apologize

Q: What’s the best way for companies to regain your trust after a hack or other data breach?
Source: PwC US Protect.me Survey, 2017
Consumers see some emerging technologies as a risk to their privacy
What emerging technologies do people see as threats to their privacy and security?

Q: How big of a threat to privacy and security is each of the following technologies?

Source: PwC US Protect.me Survey, 2017
A view from the board room
**NACD principles for cyber-risk oversight**

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Cybersecurity

Source: National Association of Corporate Directors (NACD) “Director’s Handbook on Cyber-Risk Oversight”
Cybersecurity
Questions management and boards should be asking

- Do security best practices dictate that the chief information security officer report directly to the board on a periodic basis regarding cybersecurity/privacy protection and practices?
- Is outsourcing data storage a better security system than at least most companies can securely do on their own?
- Regarding “cyber insurance,” what does it truly cover? Will an insurer refuse to cover you if they say you didn’t meet certain standards, duties and obligations?
- When does one bring an external “auditor” into the investigation?
- Do companies share breach experience/solutions with competitors so everyone learns or is this competitiveness barrier?
- Where a merger or acquisition is contemplated, is a review of the sufficiency and integrity of cyber protections necessary?
- What does a board “dashboard” look like regarding cybersecurity?
The bottom line

Companies must put cybersecurity and privacy at the forefront of business strategy to win customers’ hearts, trust—and their business. And they must implement and clearly communicate robust data governance and privacy protection policies.
5 Strategic steps to address cybersecurity risks

1. **Own the risk**
   - Cyber risk is owned by leadership and is not relegated to the IT function.
   - Periodic cybersecurity briefings are provided to the Board and C-Suite.

2. **Prioritize initiatives**
   - Leadership prioritizes and monitors cybersecurity investments.
   - Investments are made in new capability, not just technology.
   - Crown jewels have been identified and their protection prioritized.

3. **Learn and incorporate**
   - Leading organizations work with various external parties, share information on current threats and incorporate learnings into their own cybersecurity strategy and tactics.

4. **Enhance culture**
   - A security culture and mindset is established through training, measurement and evaluation.
   - Behaviors and capabilities of the organization are established and reinforce the importance of cybersecurity.

5. **Secure the business**
   - Security of the business value chain including suppliers, third party providers and high-risk interconnection points has been considered.
   - Adapt to the challenges of new and emerging digital business models.