Workshop IV

Cybersecurity: Protecting Your Business

Gary Podorowsky

Cybersecurity: Protecting Your Business

- **CHALLENGES:** The challenges of cybersecurity for small businesses
- **STRATEGIES:** Strategies to help prevent breaches of customer data and intellectual property
- **RESPONSE:** How to respond after a data breach

CHALLENGES

Personal Data Breaches and Misuse Are Continually Plaguing Consumers and Making Headlines

Facebook Role In Data Misuse Sets Off Storm – U.S. and U.K. Lash Out Over Secret Harvest
NY Times – 3/19/18

Massive Equifax data breach hits 143 million
BBC News – 9/7/17

Uber is going to have to explain to Congress why it hid the 2016 data breach that affected 57 million users
Recode – 11/27/17

Equifax Reveals An Additional 2.5 Million Data Breach Victims
WABE 90.1 FM – 3/1/18

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack
NY Times – 10/3/17

Passwords to Over a Half Million Car Tracking Devices Leaked Online
Gizmodo – 9/21/17

Massive Leak of 10 Million VIN [Vehicle Identification Numbers
Gizmodo – 6/5/17

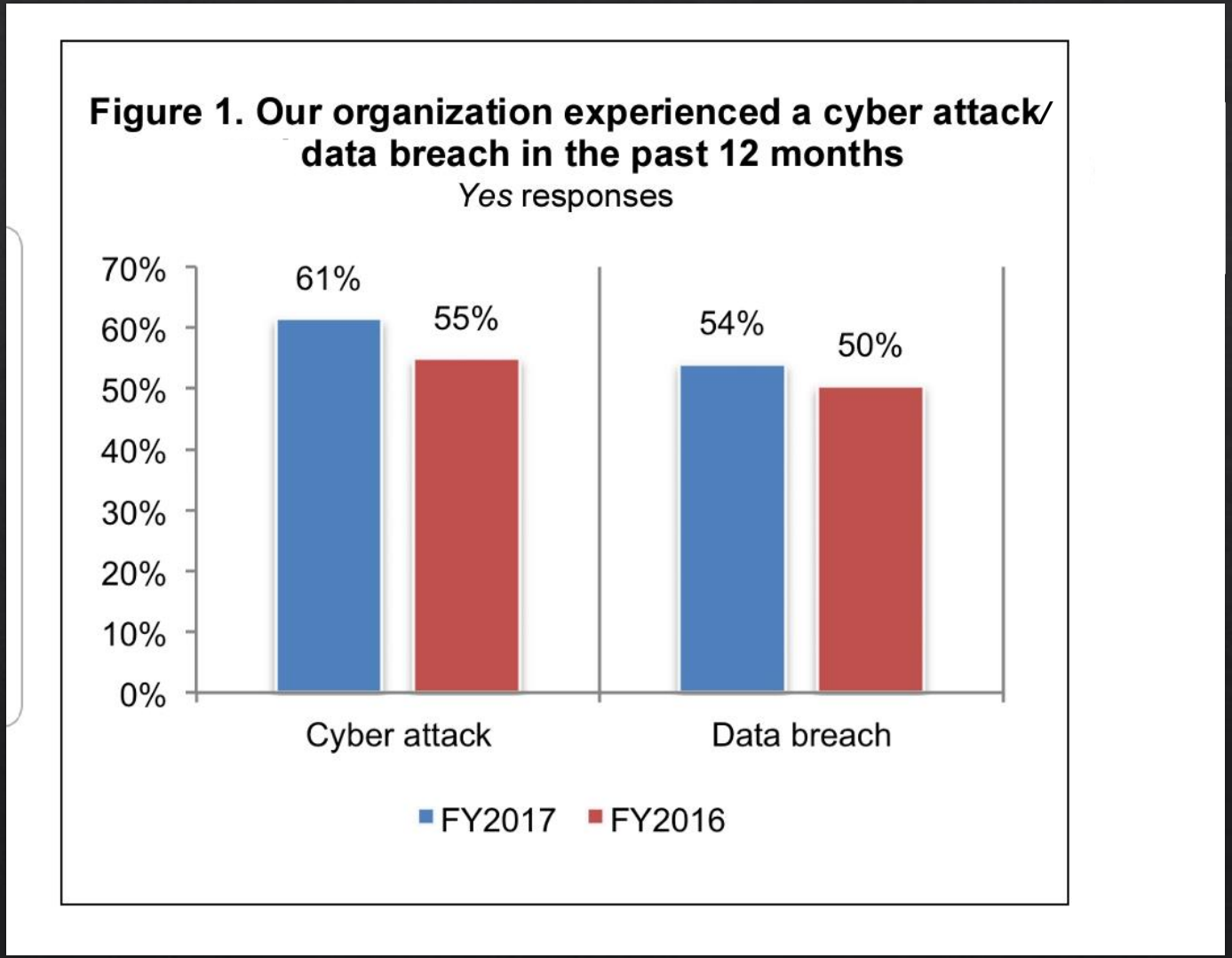
Data on 198 million voters exposed by GOP contractor
The Hill – 6/19/17

Massive ransomware infection [WannaCry] hits computers in 99 countries
BBC News 5/13/17

“There are two types of companies – those who know that they have been hacked, and those who don’t know that they have been hacked.”

John Chambers, former CEO and Chairman of the Board of Cisco Systems, Inc.

More than 60% of Small and Medium Size Businesses (SMBs) Experienced a Cyber Attack in the Past 12 Months



2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB), Ponemon Institute, September 2017

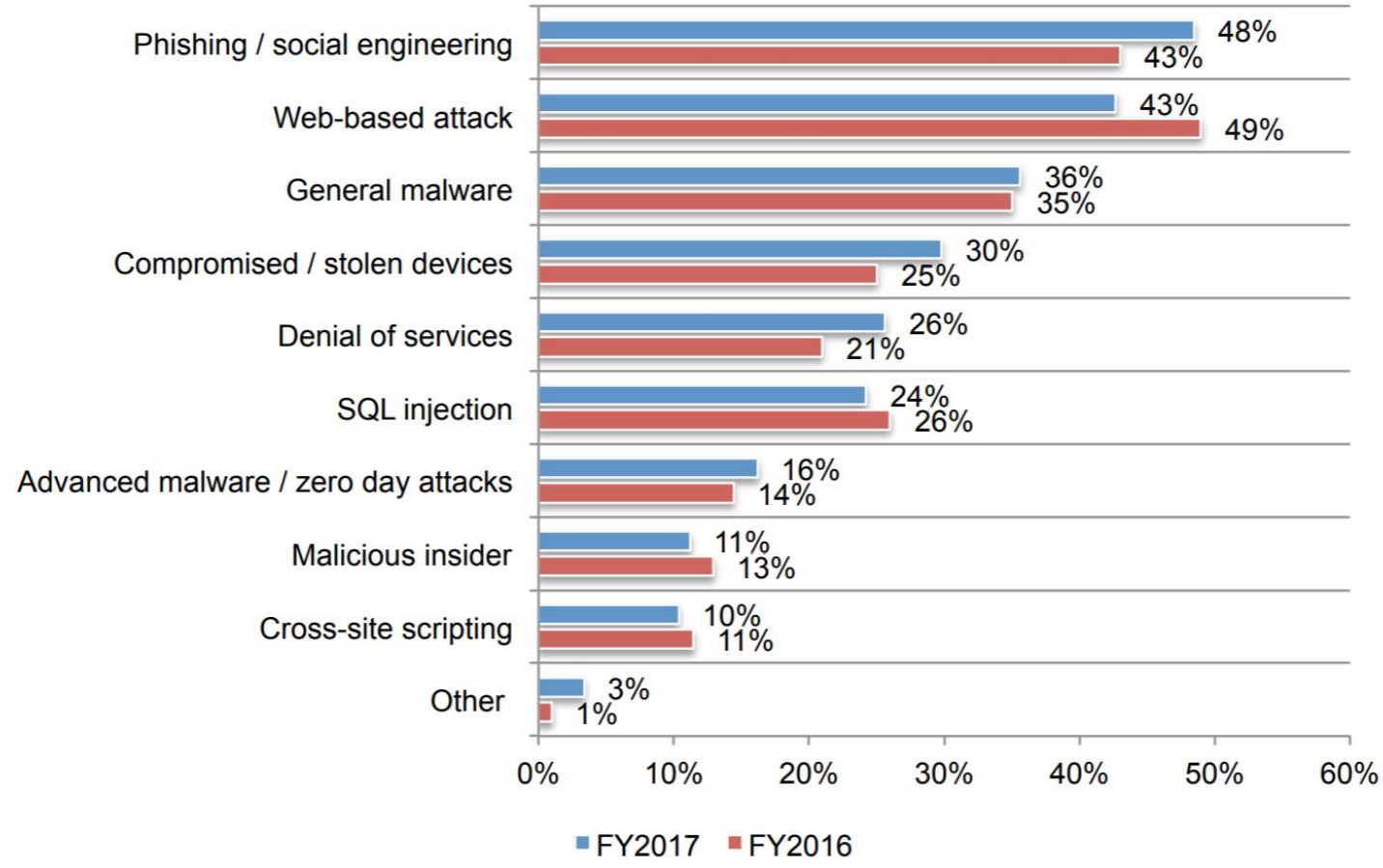
Cyber Attacks: Additional Disturbing Facts

- "Attacks are becoming costlier to business, with damage now over $1 million" average cost per incident*
- "Ransomware is hitting small and medium size businesses (SMBs) hard, with more than 50% experiencing an attack"*
- "Negligent employees are the #1 root cause behind data breaches across North America and the UK"*

* www.prnewswire.com; news provided by Keeper Security, Inc.; September 19, 2017

In 2017, Phishing and Social Engineering Became the Most Prevalent Type of Attack

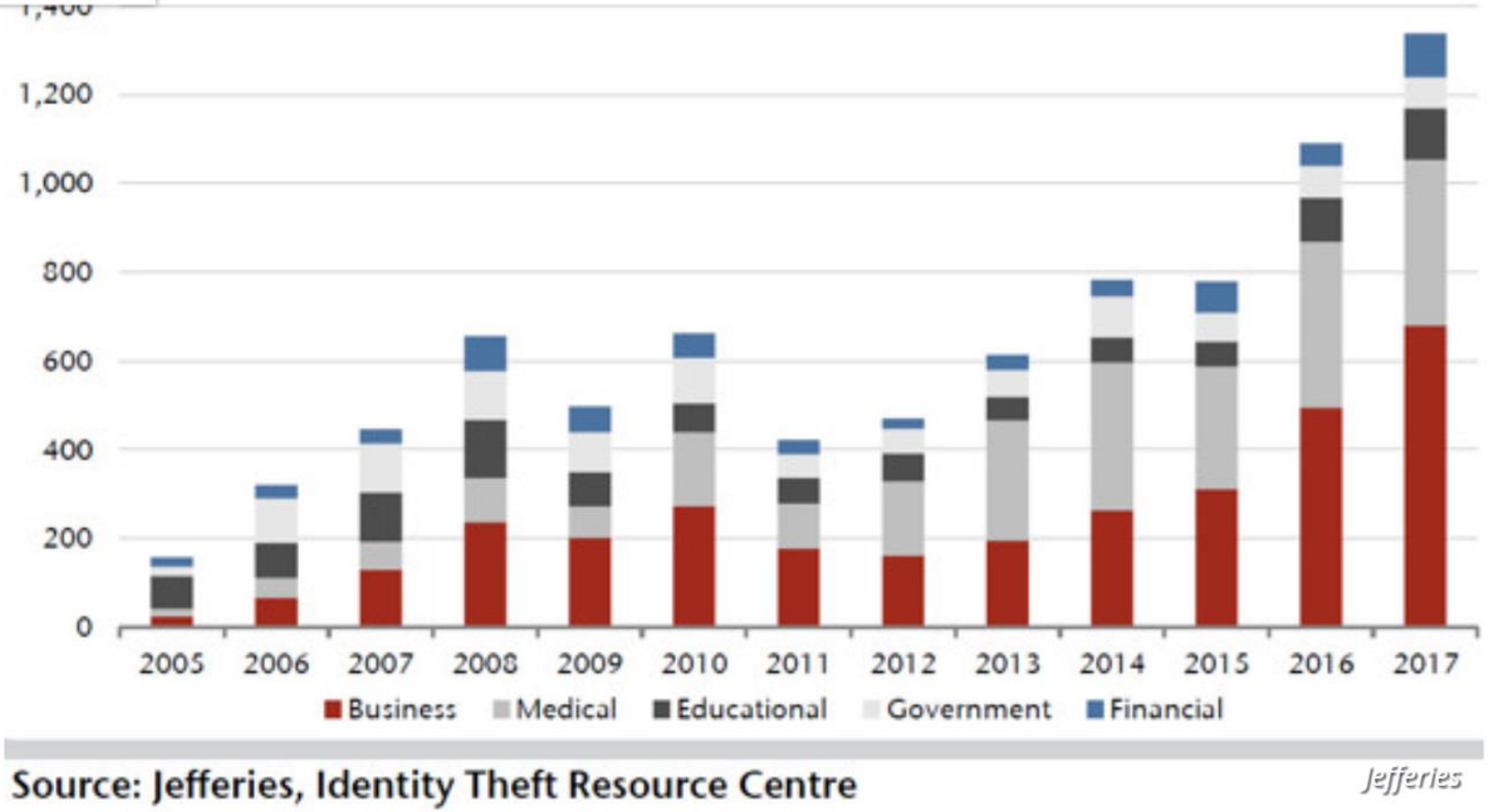
Figure 2. What types of attacks did your business experience?
More than one choice allowed



2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB), Ponemon Institute, September 2017

Another day, another data breach

MarketWatch



Source: Jefferies, Identity Theft Resource Centre

Jefferies

Here are the numbers behind the recent sharp rise in data breaches.

Cybersecurity and Privacy: Legal and Regulatory Frameworks
United States

- State Breach Notification Laws (48 states+)
- California Consumer Privacy Act (new)
- Federal Trade Commission (Section 5, Security Guidelines, Case law)

Sectoral

Marketing
- CANSPAM
- COPPA

Financial
- PCI-DSS*
- FCRA/FACTA
- Gramm-Leach-Bliley
- Dodd-Frank

Healthcare
- HIPAA
- HITECH
- GINA (Genetic Information)

Education
- FERPA

*Payment Card Industry regulation

Cybersecurity and Privacy: Legal and Regulatory Frameworks

European Union

General Data Protection Regulation (GDPR)

GDPR - New Requirements vs. European Directive
Expanded EU regulatory scope to all companies globally that process personal data about EU residents in connection with offering goods or services or monitoring EU residents' behavior
Dramatically higher penalties for non-compliance – as high as 4% of the company's global revenues
Individuals must have the Right to Be Forgotten
Requires unambiguous, active Consent (Opt-in, not Opt-Out) to process certain Personal Data
Companies must notify government supervisory authorities within 72 hours after becoming aware of a Data Breach

Cybersecurity & Privacy Challenges

1. Establishing and maintaining **adequate cybersecurity & privacy protections**, even though company resources may be quite limited
2. Protecting against **rapidly evolving threats**, both external and internal
3. Assessing and prioritizing **cybersecurity and privacy risks**
4. Understanding the cybersecurity and privacy **implications of business decisions**
5. Meeting **clients' increasing demands** for cybersecurity and privacy protection
6. Keeping up with an **evolving regulatory environment**, including expanded reach of privacy and security laws
7. Being prepared if a **serious data breach** occurs

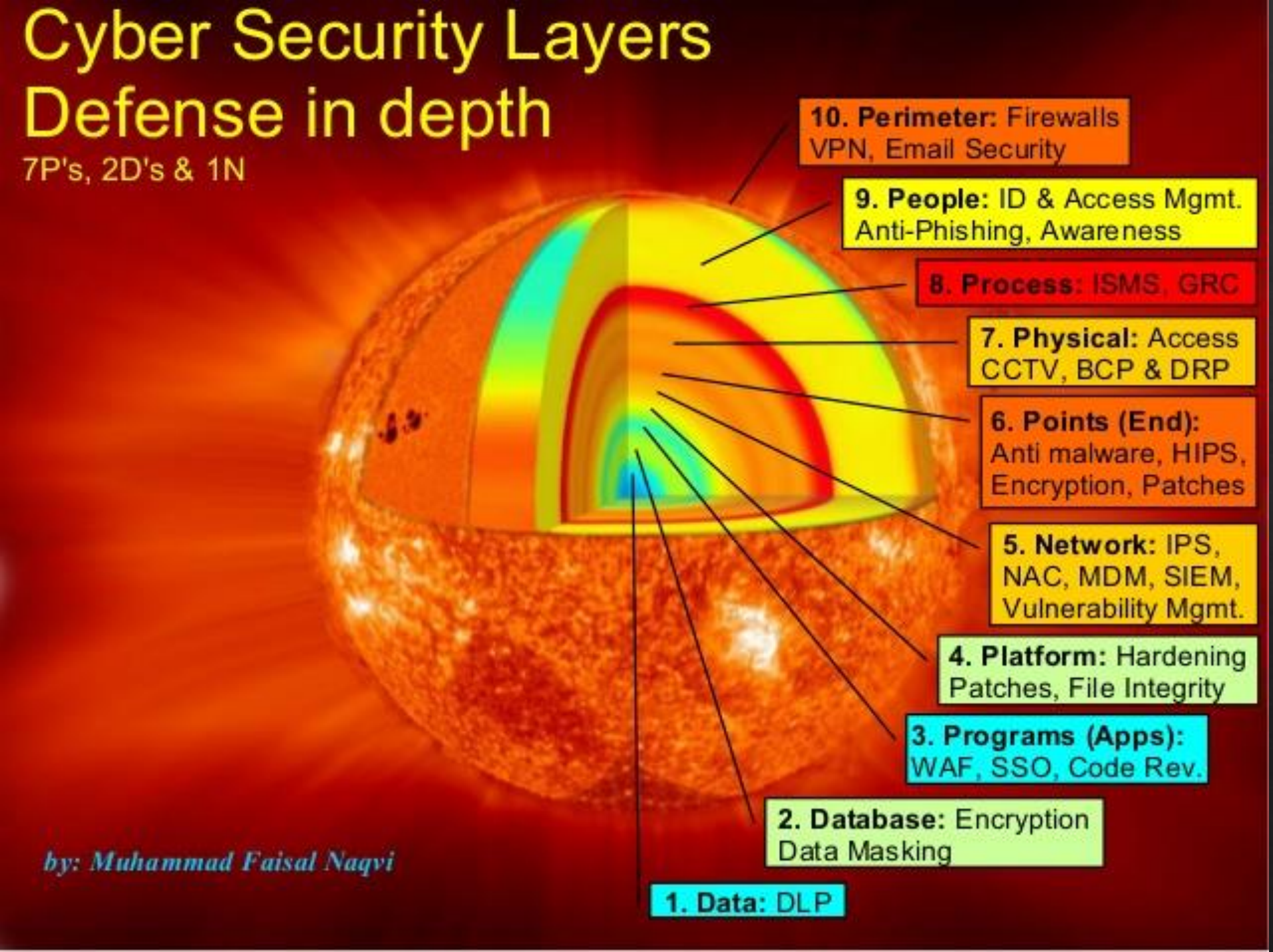
STRATEGIES TO MEET THESE CHALLENGES

What Should a Small Business Do to Protect Personal Information, Intellectual Property and Other Sensitive Data? (1)

"Perfect security is a myth" *

- Take a risk-based approach
  1. Know what information assets you have and classify them
  2. Focus heavily on protecting critical, high value and highly confidential assets, especially those facing serious threats; encrypt them if feasible
  3. Know what information security threats your company faces, and their likelihood
  4. Seek Board approval of strategy and acceptable risk level

* Source: Effective Risk Management: An Integrated Approach; Robert F. Brese; Navigating the Digital Age



Source: Muhammad Faisal Naqvi at https://www.slideshare.net/mfnaqvi?utm_campaign=profiletracking&utm_medium=sssite&utm_source=slideview

How Can a Small Company Manage All of This?

	In Large Companies	In Small Companies
Who manages cybersecurity?	Chief Information Security Officer and Information Security department; separate from IT department	Head of IT and IT staff; may supplement with external cybersecurity service; helps greatly if Head of IT has expertise in cybersecurity
Must the entire program be in place now?	Since likely collecting personal information from residents of many geographies, must have (almost) all in place now	Will depend on geographic breadth of customers and business sector breadth
How customized must plans, frameworks, tools, written documents be?	Complex systems and situations in large companies often require unique or highly customized approaches, applications and tools.	With less complexity, it is often feasible to use well-known, highly-rated and secure, standard solutions/tools
Use internal staff or outsourced staff	May select either approach. May build and operate own Security Operations Center (SOC) and Security Information and Event Management (SIEM)	Outsource many functions (e.g., Managed Detection and Response (MDR) Service, Vulnerability/Penetration Testing), but manage the vendors.

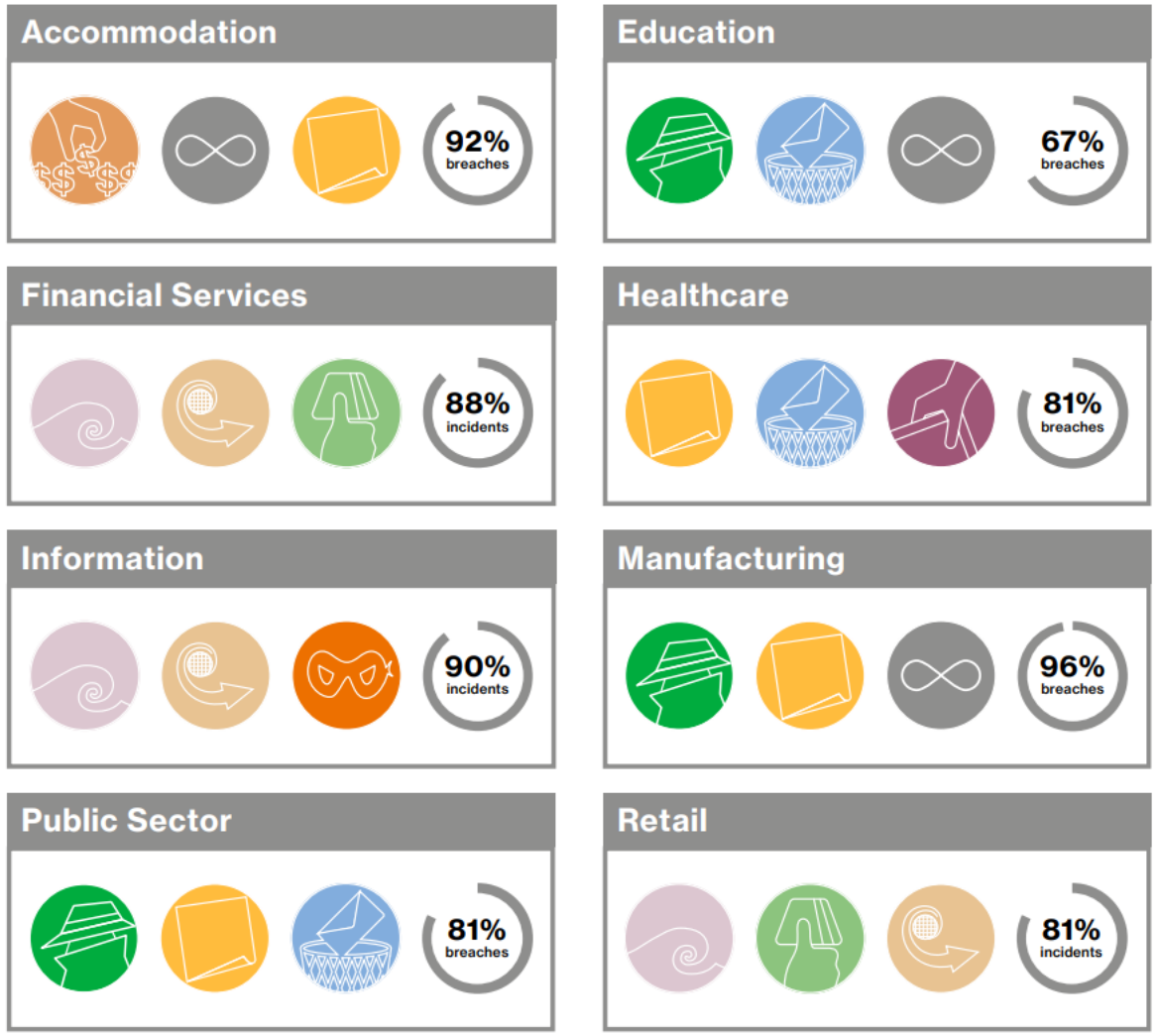
Indicators of Degree of Security & Privacy Needed

- Value of Intellectual Property (IP)?
- Competitiveness of industry?
- Sensitivity and value of personal information collected/processed?
- Personal Health Information collected/processed?
- Personal Information of Children under 13 collected/processed?
- Credit Card Data collected/processed?
- Collect/process Personal Information/IP as agent for large corporation?
- Company's risk tolerance?

file:///C:/Users/Gary/Downloads/rp_DBIR_2017_Report_execsummary_en_xg.pdf

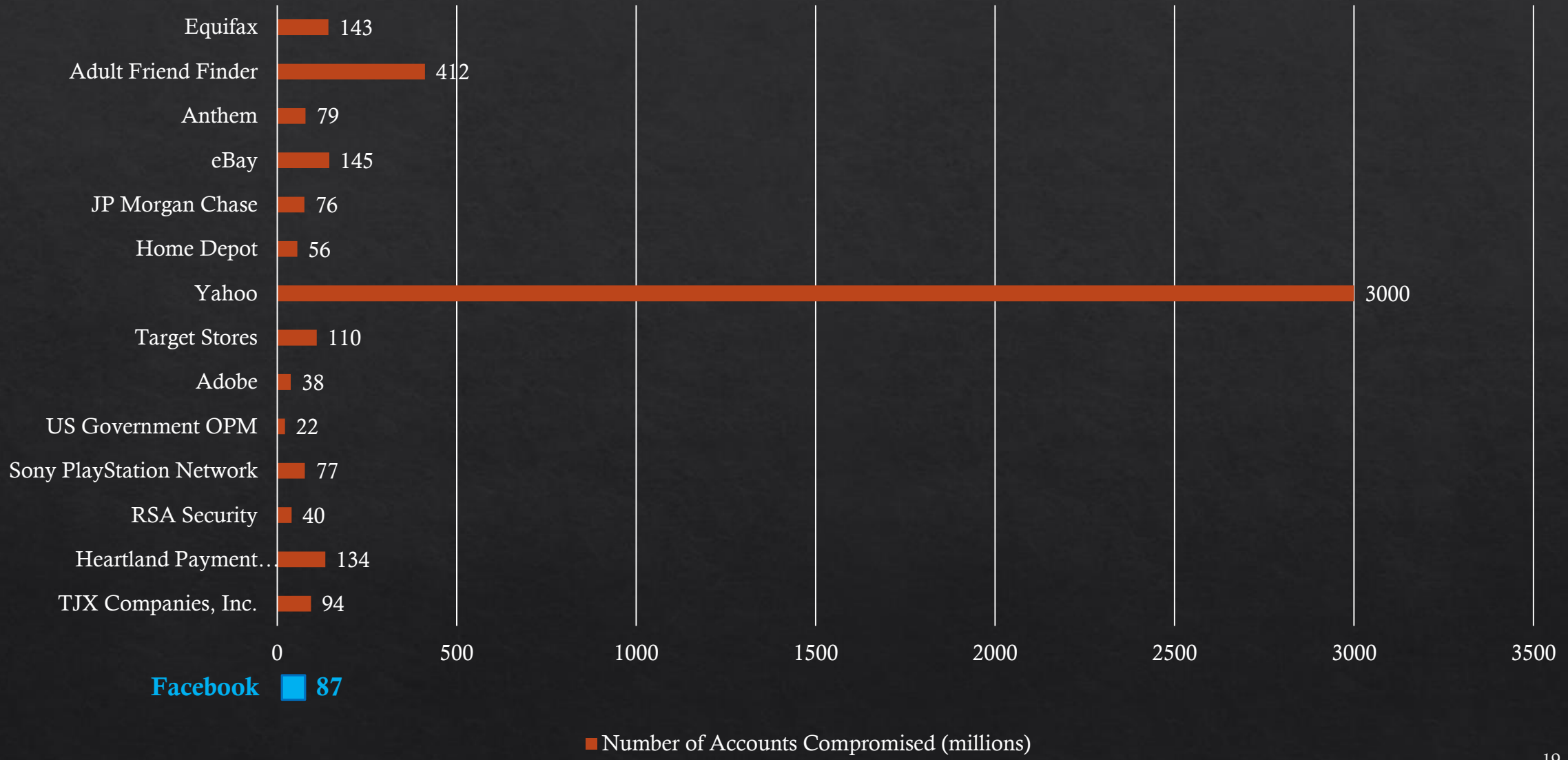
- Payment card skimmers
- Point of sale intrusions
- Denial of service
- Insider and Privilege misuse
- Everything else

Know the Threats you Face



- Crimeware
- Web application attacks
- Cyber espionage
- Physical theft & loss
- Miscellaneous errors

The 14 Biggest Data Breaches of the 21st Century*



*Through December 31, 2017; based on number of accounts compromised

Source: "The 17 biggest data breaches of the 21st century", Taylor Armerding, CSO (Chief Security Officer) magazine, January 26, 2018

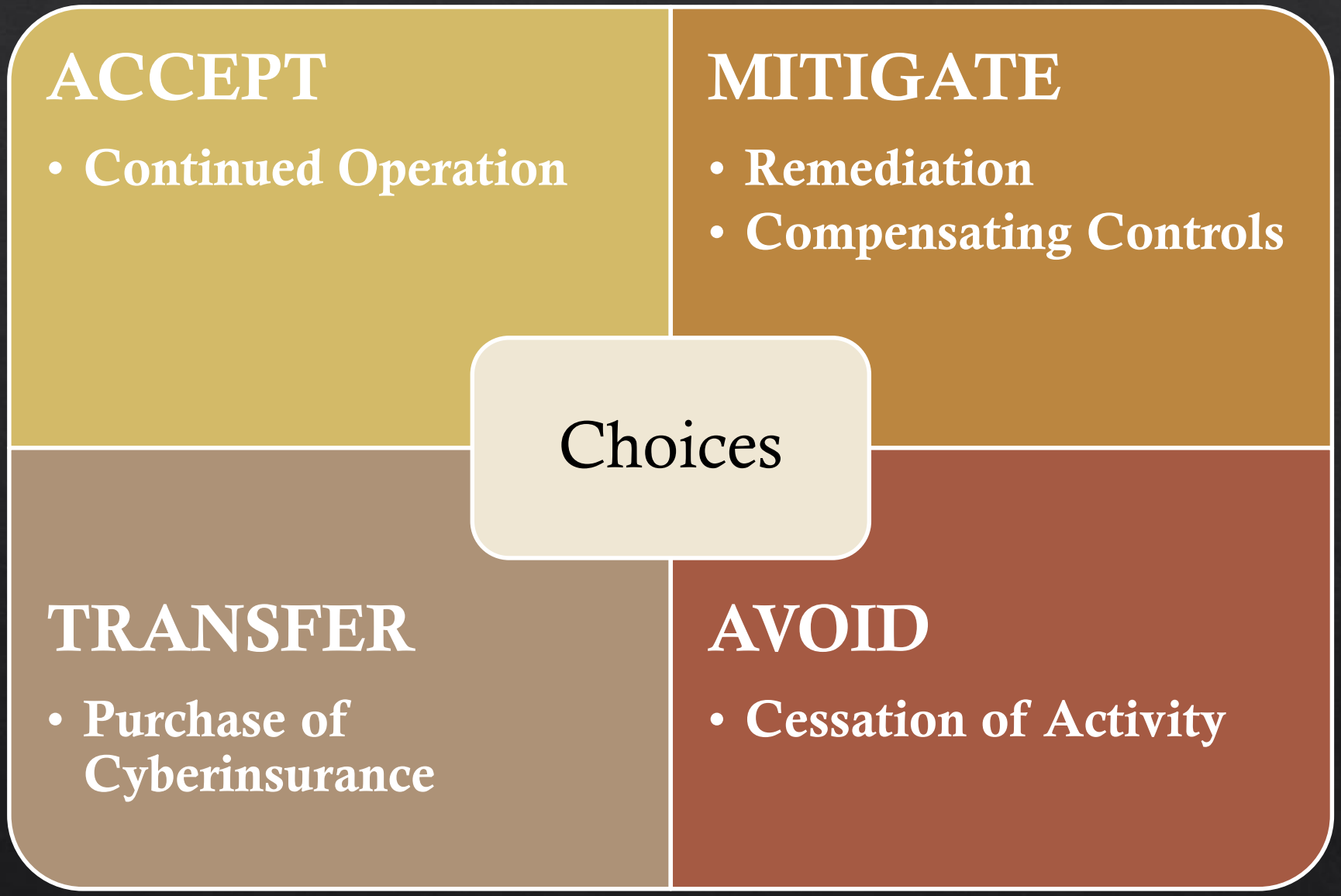
Learn from the FAILURES that Made Major Breaches Possible

Company Breached	Company Failure that Contributed to Breach
Equifax	Equifax had not yet patched Apache Struts vulnerability due to insufficient or inaccurate inventory of server applications.
Target	Target did not focus on the information security status of some of its vendors that had access to Target's network. As a result, hackers were able to get into Target's point-of-sale system by way of vulnerabilities in Target's HVAC contractor's software.
Yahoo	Yahoo did not invest enough in its information security program to prevent or detect multiple hackings of its vast customer databases.
Anthem	Anthem did not encrypt sensitive customer personal information, thus making the data vulnerable if breached.
Facebook	Facebook did not know what its business partner was doing with the customer personal information it allowed the partner to access.

“Acceptance of cybersecurity risks is a business decision senior executives will be called to make.”*

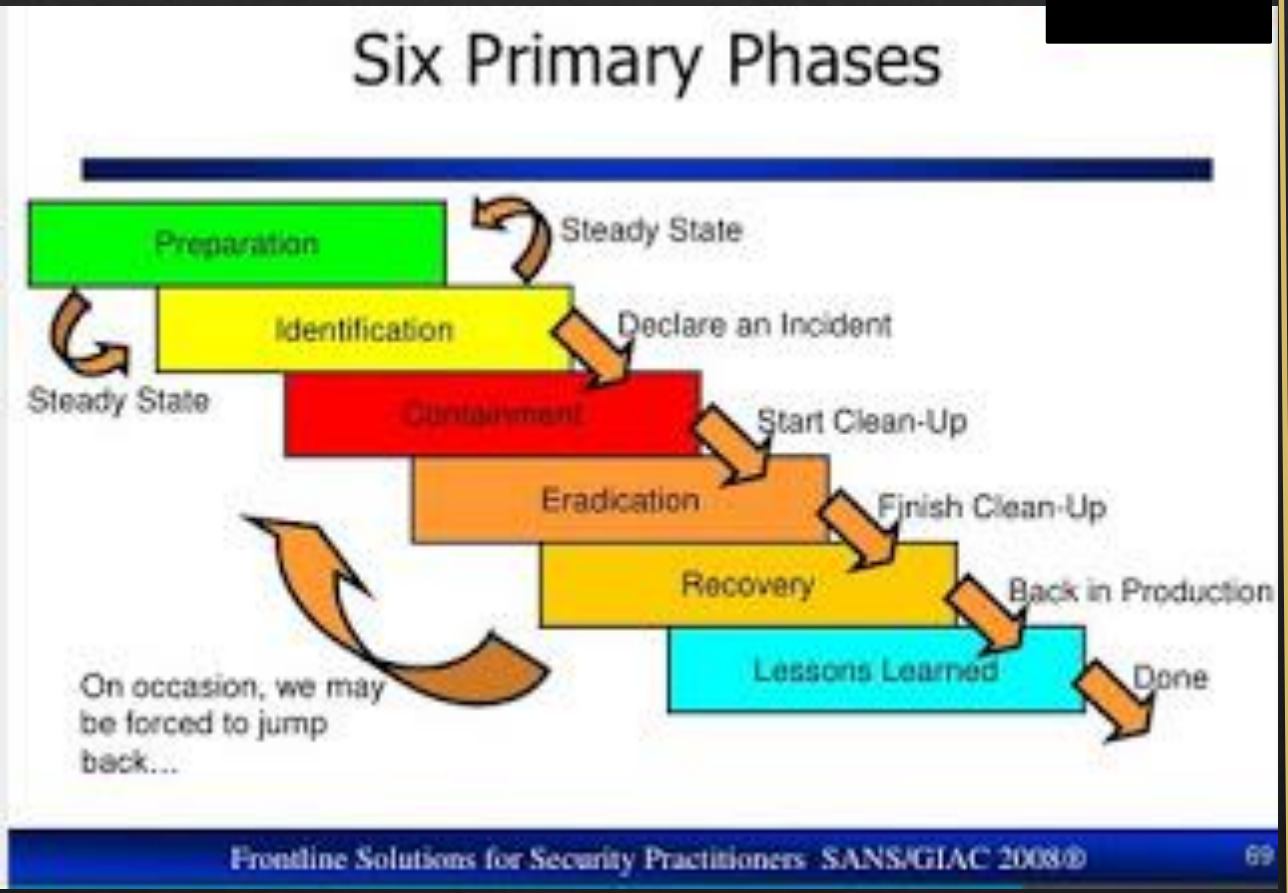
*** Source of the quote: Cybersecurity for Executives – A Practical Guide, page 73**

A Risk-based Approach: Four Choices in Addressing Risks



BREACH RESPONSE

Incident Response – Technical Steps



RESPONDING TO AN INCIDENT

1 PREPARATION
- Policies, procedures and guidelines
- Document and practice incident response process
- Determine roles, responsibilities and communication plans

2 IDENTIFICATION
- Recognition and reporting of event
- Determine if the event is an incident

3 CONTAINMENT
- Stop the spread
- Secure and protect vital information systems

4 ERADICATION
- Identify root cause of incident and negative effects
- Remove the root cause
- Identify all weaknesses that led to incident

5 RECOVERY
- Restore affected systems
- Test and validate systems for correct functionality
- Restore business operation

6 REVIEW & IMPROVE
- Debrief following incident recovery
- Fix identified weaknesses
- Update and improve incident response process

©2015 Kalki Consulting LLC
17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554

KALKI

Key Actions for a Rapid and Effective Data Breach Response*

1. **Activate** Data Breach Response Plan
2. **Activate** pre-negotiated agreements
3. **Identify, Contain and Eradicate** the malware, intrusion, etc.
4. **Preserve** evidence
5. **Determine** the scope and specific elements of data accessed/stolen
6. **Develop and issue** a statement about what has happened
7. **Identify and address** legal requirements (e.g., notifications)
8. **Notify** cyber insurance company
9. **Take** necessary actions to restore or continue business operations
10. **Deploy** Business Continuity Plan if necessary

* The optimal order of these steps will depend on the specific situation. Some steps may be concurrent. All must be coordinated and agreed by the breach management team.

Examples of Challenges in Data Breach Response

1. **Investigating the breach** without corrupting evidence
2. **Determining the path of intruders** who erased their footprints
3. **Determining the jurisdictions** of the persons affected by the data breach
4. **Issuing a statement** about the breach that is accurate, sufficient and timely
5. **Using data breach response plans** that likely were not sufficiently tested
6. **Using a business continuity plan** that may not have determined Recovery Time Objectives for many applications
7. **Scaling up customer service** for response speed, accuracy and sufficiency
8. **Unpredictable path** of a cyber crisis

Cyber Insurance

- Risk decision based on the potential impact and likelihood of a breach of sensitive personal information, the company's risk tolerance, premiums, etc.
- Coverage from policies other than the Cyber Insurance Policy
  - Exclusions from Property and Casualty/Umbrella Liability policies
- Government-sponsored attacks
- Challenges of renewing Cyber Insurance after a breach

CONFIDENTI
AL

Key Actions and Expertise of the Forensics Investigation Firm

- "Handle critical security incidents, resolve immediate issues and put solutions in place to address systemic causes of the incident"
- "… expertise and intelligence that enables its consultants to identify the actions of the attacker, the scope of the compromise and what data was lost …"
- "Investigative skills … Threat intelligence … Technology … Law enforcement relationships … Management experience … Dedicated malware team"

Source: www.fireeye.com

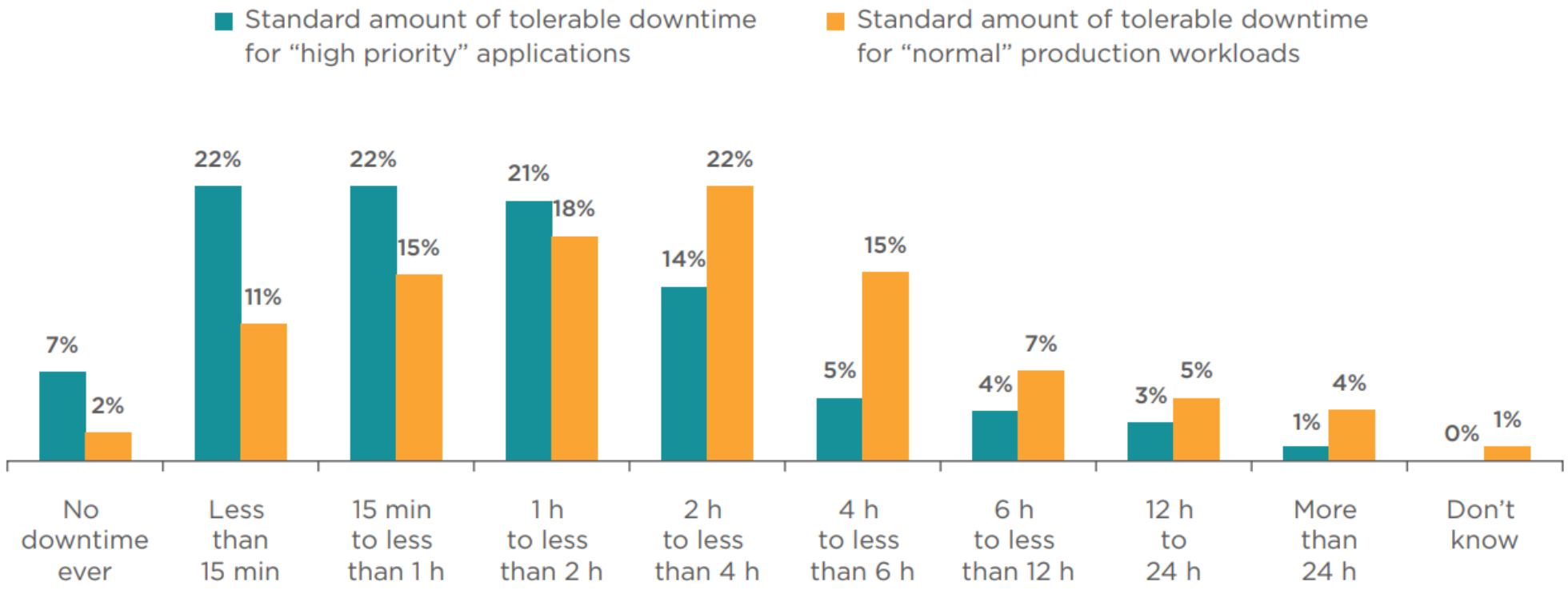
Key Actions of the External Cyber Breach Law Firm

"Cyberattack investigations require a team of lawyers with regulatory, data-breach response, privacy, litigation, and eDiscovery expertise"

1. **Provide advice and/or take steps directly to preserve evidence**
2. **Provide legal advice on reporting and other legal and regulatory requirements**
3. **Secure Attorney-client Privilege where feasible**
4. **Review breach response statements**
5. **Act as a liaison to Law Enforcement**

Source: "Forensic remediation" ; Jim Jaeger and Ryan Vela; Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers; PaloAlto and NYSE; 2015; chapter 36

Amount of Downtime Organizations Can Tolerate



Source: *ESG Research Report, The Evolving Business Continuity and Disaster Recovery Landscape*, February 2016.

Unpredictable path of a cyber crisis

- Physical threats to company operations, management, other employees, and/or customers
- Publication of sensitive information of customers, officers, employees, shareholders (not only expected information)
- Pre-cursor to, and distraction from, the “real” attack
- Prompt to other hackers to sense vulnerability and to launch attacks

Suggested Reading

1. **Cybersecurity for Executives: A Practical Guide**; Gregory J. Touhill, C. Joseph Touhill; Wiley, 2014
2. **Cybersecurity for Small Businesses and Nonprofits**; Jane LeClair, Denise Pheils & Carolyn Schrader; Excelsior College/Excelsior College's National Cybersecurity Institute (NCI); 2016
3. **2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)**; Ponemon Institute; Sponsored by Keeper Security; September 2017 https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html
4. **2018 Verizon Data Breach Investigations Report (DBIR): Tales of Dirty Deeds and Unscrupulous Activities**; www.verizonenterprise.com/verizon-insights-lab/dbir/; Verizon Enterprise Solutions; 2018
5. **Start with Security: A Guide for Business**; U.S. Federal Trade Commission; https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
6. **"The Best Practices in Cyber Security for Small-to-Medium-Sized Businesses"**; Kate Harrison, contributor; Forbes; May 3, 2016

Thank you!

Questions?

Email: Gary.Podorowsky@gmail.com