Computer, Network & Internet Security:

What you should know and what you can do to defend your business and yourself

10/1/2015

Presented by: Dan Gibson, Jerry Ravi, Bill Blum

ALPINE BUSINESS SYSTEMS, INC.

EISNERAMPER

Webinar Introduction

- We are pleased to welcome you to today's webcast. In order to qualify for your CPE Certificate, you will need to:
  - Remain logged on for at least **50** minutes
  - Respond to at least **3** of the **4** polling questions that will be presented
- We would appreciate if you would complete the evaluation survey following the event. A link to the survey will be emailed to you automatically within the hour following the webinar.
- You may submit questions and we will try to address them during the program. However, if time does not permit us to answer a question posed during the webcast, it will be answered offline after the event.

CPE Certificate Information

- For those who meet the criteria, a CPE certificate will be deposited into your Checkpoint Learning account. Our activity history and CPE certificates are now managed using Checkpoint Learning. In order to receive CPE credit for this program, you must register for a Checkpoint Learning account through our Executive College before the webinar begins.
- To apply for a complimentary account visit the Executive College page at www.eisneramper.com. CPE certificates will be distributed into your Checkpoint Learning account 10-14 business days AFTER the webinar.
- Disclaimer: We may be unable to offer CPE certificates to people who log in to the webinar using:
  - Google Chrome
  - GoToWebinar **Instant Join**
  - iPads or mobile devices

These login methods may prevent you from being registered on the final attendee report. To ensure that you show up on the final attendee report, please log in using a different method than the ones listed above.

Speakers

Dan Gibson
Partner
EisnerAmper LLP
Daniel.Gibson@eisneramper.com

Jerry Ravi
Partner
EisnerAmper LLP
Jerry.ravi@eisneramper.com

Bill Blum
President
Alpine Business Systems
bblum@alpinebiz.com

Cybersecurity is Everyone's Business

- President Obama designated October 2015 **National Cyber Security Awareness Month**
- **http://www.dhs.gov/national-cyber-security-awareness-month**
- The fifth anniversary of "**Stop. Think. Connect.**"
- This week focuses on cybersecurity as a shared responsibility

Session Objective

Security breaches have had a profound impact on the C-Suite and Boardroom.

Key takeaways:

- Where we are today?
- How are companies approaching cybersecurity risk management?
- How to do we implement and leverage a continuous monitoring process?
- How to establish an incident response process?

The “Current State” of Cyber Threats

Innovation & Next Generation Technology

- Big Data, Outsourcing, Cloud Computing, Mobile Devices
- Most, if not all, industries are exposed
- EVERYTHING IS CONNECTED!

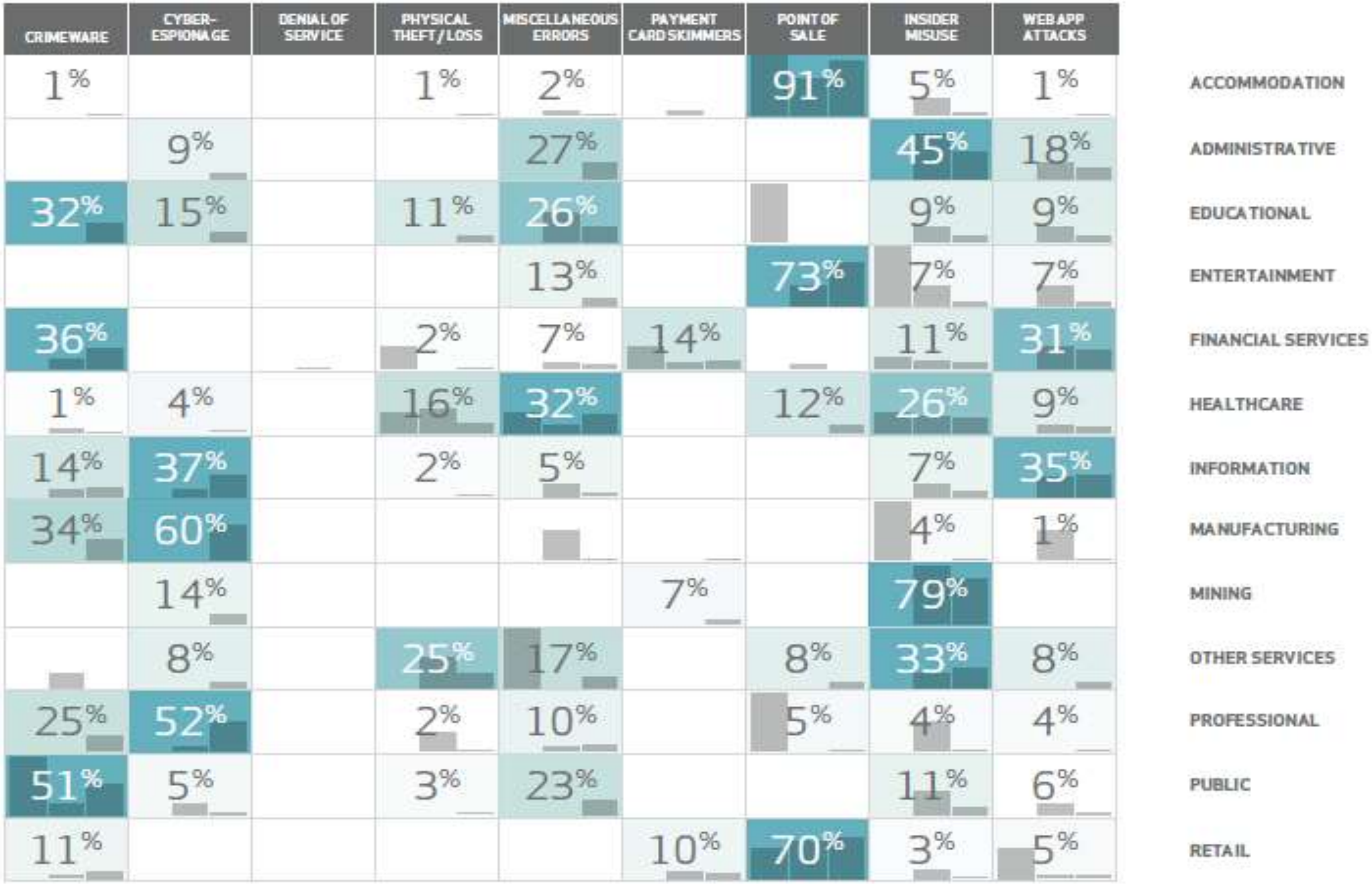
Tightening Regulation

- National Security Mandate
- SEC Alerts / Disclosures
- Banking & Insurance Regulators: Cyber now part of their examination procedures

REPUTATIONAL RISK

WE ALL HAVE CYBER *INSECURITY*!!!!

Frequency of Breach Type by Industry



CRIMEWARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	PHYSICAL THEFT/LOSS	MISCELLANEOUS ERRORS	PAYMENT CARD SKIMMERS	POINT OF SALE	INSIDER MISUSE	WEB APP ATTACKS	
1%			1%	2%		91%	5%	1%	ACCOMMODATION
	9%			27%			45%	18%	ADMINISTRATIVE
32%	15%		11%	26%			9%	9%	EDUCATIONAL
				13%		73%	7%	7%	ENTERTAINMENT
36%			2%	7%	14%		11%	31%	FINANCIAL SERVICES
1%	4%		16%	32%		12%	26%	9%	HEALTHCARE
14%	37%		2%	5%			7%	35%	INFORMATION
34%	60%						4%	1%	MANUFACTURING
	14%				7%		79%		MINING
	8%		25%	17%		8%	33%	8%	OTHER SERVICES
25%	52%		2%	10%		5%	4%	4%	PROFESSIONAL
51%	5%		3%	23%			11%	6%	PUBLIC
11%					10%	70%	3%	5%	RETAIL

The top three industries affected are the same as previous years: Public, Information, and Financial Services.

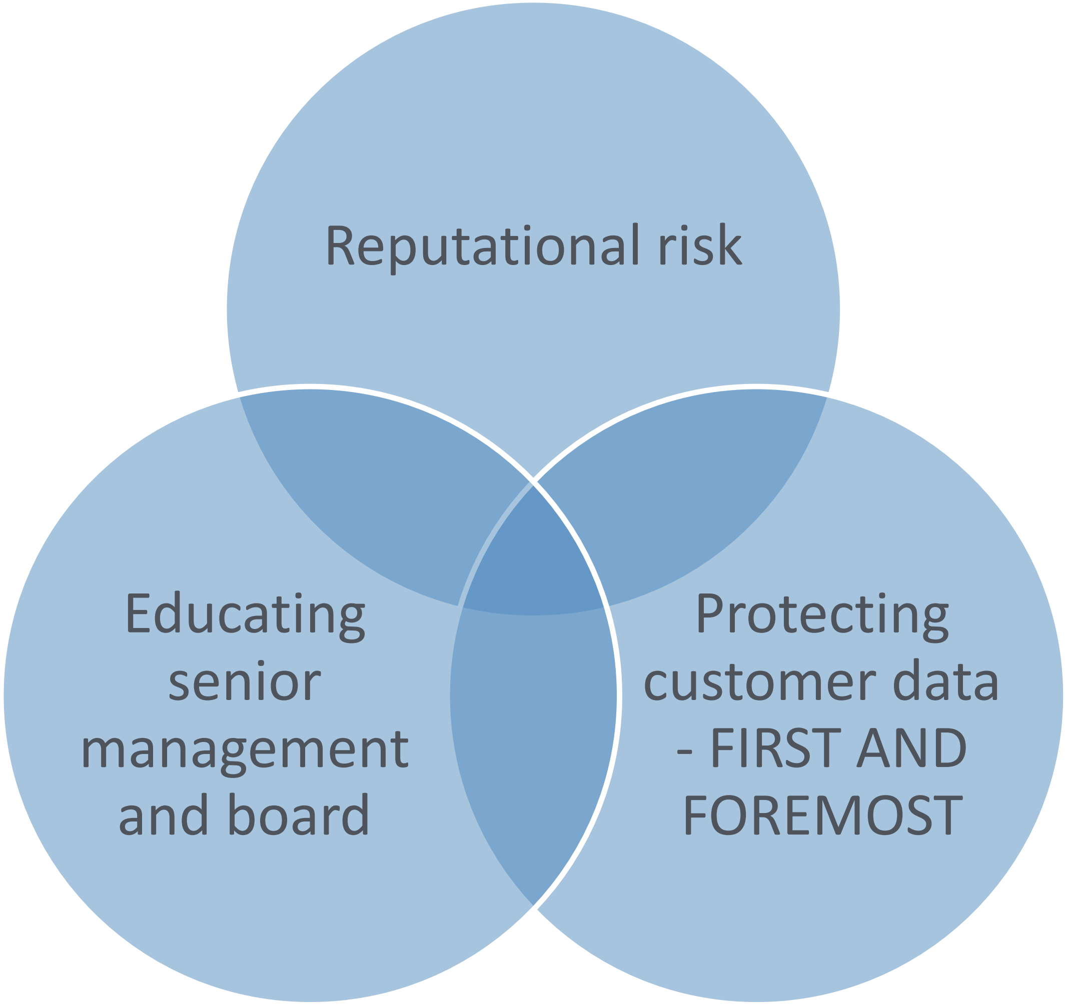
Polling Question #1

Have the publicized security breaches over the past year caused a heightened alertness for cybersecurity within your company?

A. Yes

B. No

Key Considerations: CFO / Board Perspective



Reputational risk

Educating senior management and board

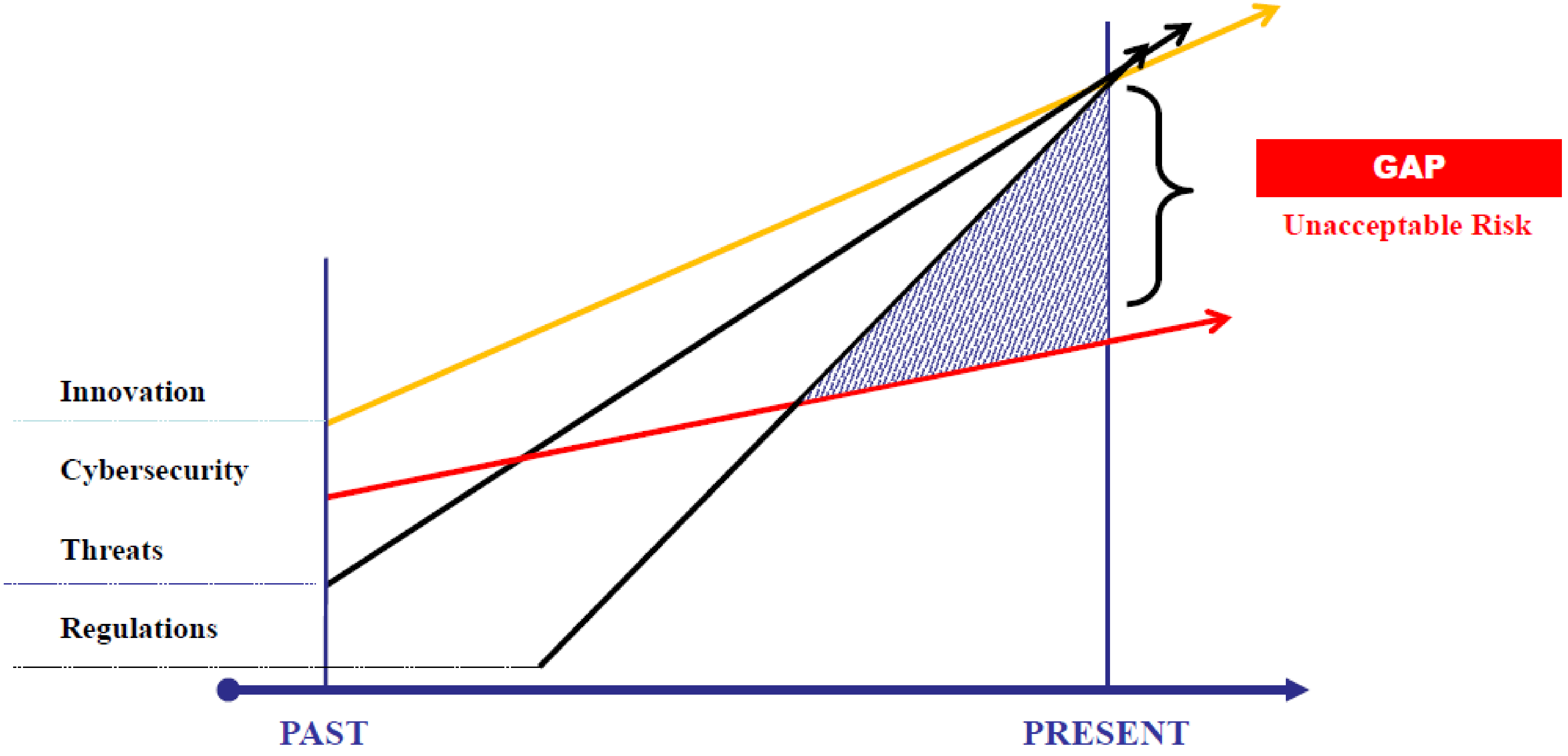
Protecting customer data - FIRST AND FOREMOST

5 Principles of Cybersecurity for Board Members

- PRINCIPLE 1
  - **Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.**
- PRINCIPLE 2
  - **Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.**
- PRINCIPLE 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.**
- PRINCIPLE 4
  - **Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.**
- PRINCIPLE 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.**

NACD®
NATIONAL ASSOCIATION OF
CORPORATE DIRECTORS

The "Current" Cyber Risk Landscape



Courtesy – CGI Cybersecurity

Building Your Cyber Literacy

Challenges

- Having a plan and executing?
- Over reliance on C-Suite and Third Party Providers
- How do you track progress and who gets involved?

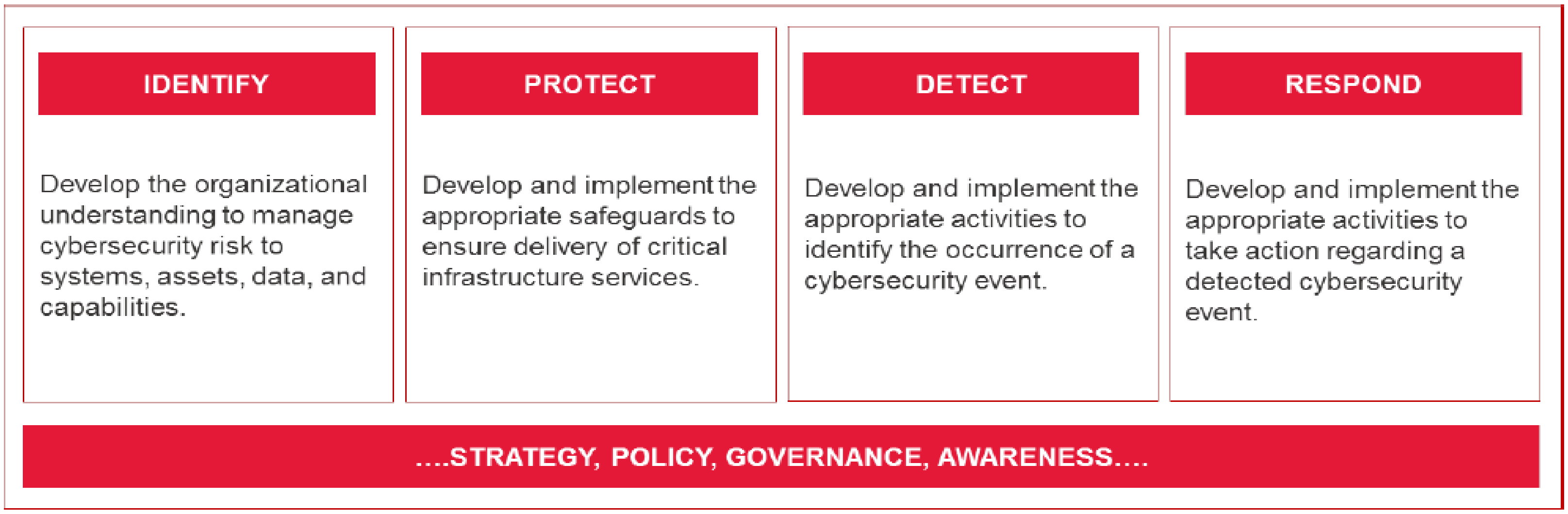
Action Items

- Ask questions
- Champion Risk Assessment activities
- Make cyber part of the communication process (your vocabulary)
- Using Metrics and Assurance / Assessment Activities (internal audit or internal / external reviews)

Creating a Modern Security Program

There are four major categories of dealing with risk:

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)



IDENTIFY

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

PROTECT

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

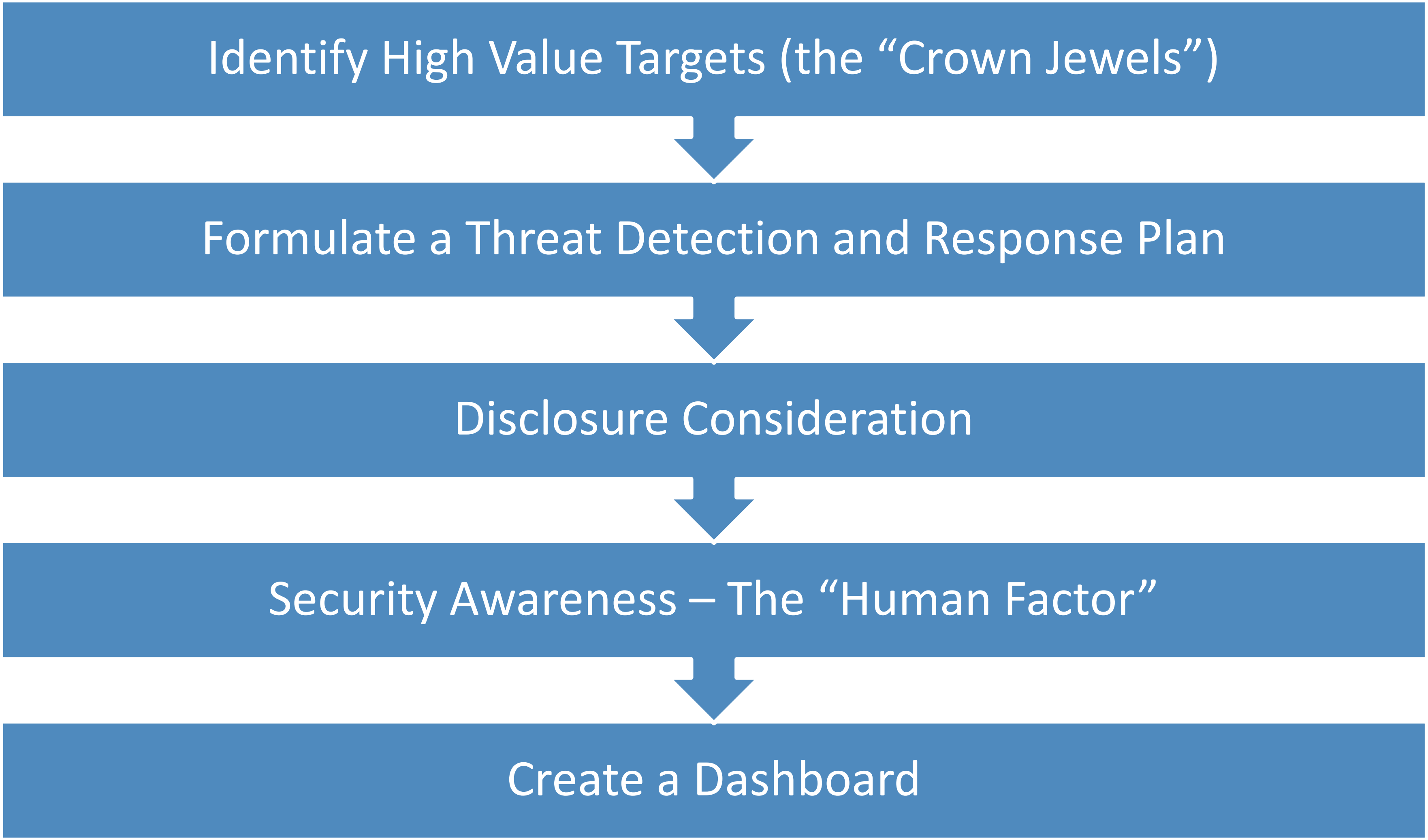
RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

....STRATEGY, POLICY, GOVERNANCE, AWARENESS....

Courtesy – CGI Cybersecurity

Key Considerations for Board: Management Dialogue



Identify High Value Targets (the “Crown Jewels”)

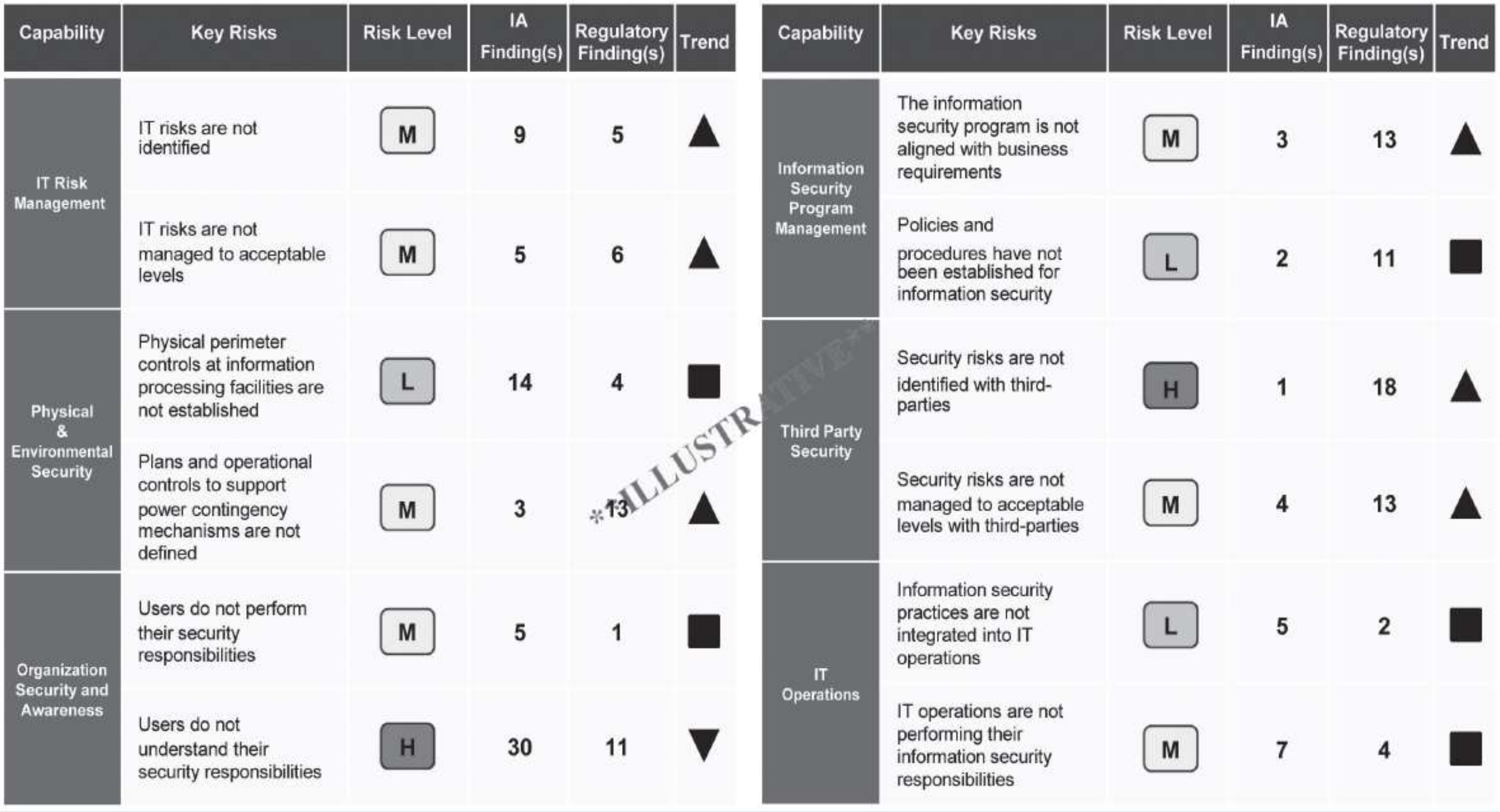
Formulate a Threat Detection and Response Plan

Disclosure Consideration

Security Awareness – The “Human Factor”

Create a Dashboard

Example: Board / Executive Risk Dashboard



Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
IT Risk Management	IT risks are not identified	M	9	5	▲
	IT risks are not managed to acceptable levels	M	5	6	▲
Physical & Environmental Security	Physical perimeter controls at information processing facilities are not established	L	14	4	■
	Plans and operational controls to support power contingency mechanisms are not defined	M	3	13	▲
Organization Security and Awareness	Users do not perform their security responsibilities	M	5	1	■
	Users do not understand their security responsibilities	H	30	11	▼

Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
Information Security Program Management	The information security program is not aligned with business requirements	M	3	13	▲
	Policies and procedures have not been established for information security	L	2	11	■
Third Party Security	Security risks are not identified with third-parties	H	1	18	▲
	Security risks are not managed to acceptable levels with third-parties	M	4	13	▲
IT Operations	Information security practices are not integrated into IT operations	L	5	2	■
	IT operations are not performing their information security responsibilities	M	7	4	■

Source: NACD Cyber Director's Handbook

Cybersecurity: Questions to Ask

Management can ask the following questions:

1. Does your organization use a security framework?
2. What are the top 5 organizational risks related to cybersecurity that your company is faced with?
3. How are your employees made aware of their role related to cybersecurity?
4. Are external and internal threats considered when planning your cybersecurity program?
5. How is security governance managed within your organization?
6. In the event of a serious breach, has management developed an effective response protocol and educated your organization?

Cyber Prep Checklist

Before an Incident or Attack

- Identify mission critical data and assets (*i.e.*, your “Crown Jewels”) and institute tiered security measures to appropriately protect those assets.
- Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.
- Create an actionable incident response plan.
  - Test plan with exercises
  - Keep plan up-to-date to reflect changes in personnel and structure Have the technology in place (or ensure that it is easily obtainable) that will be used to address an incident.
- Have procedures in place that will permit lawful network monitoring.
- Have legal counsel that is familiar with legal issues associated with cyber incidents
- Align other policies (*e.g.*, human resources and personnel policies) with your incident response plan.
- Develop proactive relationships with relevant law enforcement agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may require in the event of an incident.

Cyber Prep Checklist

During an Attack

- Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.
- Minimize continuing damage consistent with your cyber incident response plan.
- Collect and preserve data related to the incident.
  - "Image" the network
  - Keep all logs, notes, and other records
  - Keep records of ongoing attacks
- Consistent with your incident response plan, notify—
  - Appropriate management and personnel within the victim organization should
  - Law enforcement
  - Other possible victims o Department of Homeland Security
- Do not—
  - Use compromised systems to communicate.
  - Hack back" or intrude upon another network.

After Recovering from a Cyber Attack or Intrusion

- Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.
- Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan.

Polling Question #2

Do you believe cybersecurity breaches threatening your business come from:

A. Within the US

B. Outside of the US

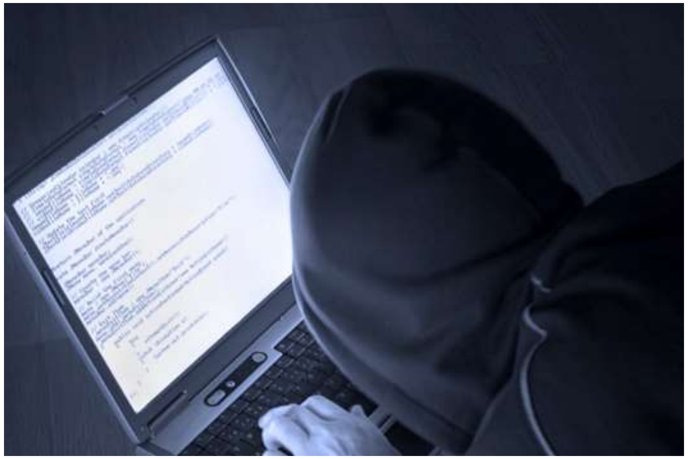
C. I don’t feel like we have a cybersecurity threat.

Important Concepts

- Backups, Disaster Recovery, and Business Continuity: Job #1
- There is no privacy on the Internet
- Information and data about you and your firm is easily accessible
- Nothing is free
- Be vigilant always

Privacy

- There is no expectation of privacy on the internet.
- The only way to be totally secure is to stay unconnected to anything.



Easy Access to Personal Information and Data

- What do Apple, Google, Microsoft, AOL, Facebook, your ISP, and the government know about you?

- EVERYTHING!
  - Your IQ
  - Personal interests
  - Browsing history
  - Habits
  - Likes, dislikes

Nothing is Free

- Forget this at your own risk
- Criminals want you to believe otherwise
- Cybercriminals make offers that are way too good to be true
  - Free music, videos
  - Free money
- What you give up for free technology

Be Vigilant Always

- The criminals never sleep – they have robots
- “Only the Paranoid Survive,” Andy Grove
  - Co-founder and CEO of Intel
- FBI reports that every company is under attack and there are only 2 kinds of companies:
  - Those that know they are under attack
  - Those that don’t

Short History of Cybercrime

- 2007 – Self morphing viruses
- 2009 – The Zeus virus, “Man in the browser” attacks and no browser is safe
- 2011 – 300% increase in cyberattacks
- 2013 – Attacks targeted at contents of RAM (Target)
- 2014 – SSL Vulnerability (Heartbleed), Sony hack
- 2015 – Massive attack at U.S. Office of Personnel Management

The Perpetrators

- Who are they?
  - Used to be pranksters, smart kids that were bored
  - State sponsored terrorists
  - Very well organized criminal networks
- Why?
  - Willie Sutton and John Dillinger knew
- Who are the targets?
  - Everyone
  - 90% of all attacks are against business with less than 1,000 employees
  - 1/3 of all breaches are against companies with < 100 employees

The Magnitude of their Success and Threat

- If "Hackers Inc." was a company:
  - #1 on Fortune 500, 74x the size of Walmart

- In 2014, 47% of American adults had their personal information stolen by hackers, primarily through data breaches at large companies (http://www.cbs.com/)

- Average total cost of a breach: $3.8 million (Source: http://www-03.ibm.com/security/data-breach/)

Criminal Methods and Techniques

- Spam
  - 98% of all email is spam

- Viruses, Spyware, and other Malware
  - Thousands caught in your filters every day

- Easy to create
- Easy to spoof email addresses
- Multiple methods of infection (emails, web sites, peer-to-peer sharing sites)

Criminal Methods and Techniques

- "Drive-by" Infections
  - 1 in 8 web pages are infected
    - Approximately 9,500 new ones every day (Google statistic)
  - Always look for the name right before .com or .org in the URL
- Phishing Techniques
  - Web Searches, E-mails or IM's impersonating a trusted entity
  - Directs you to a phony web site, then look out!

Polling Question #3

Have you been targeted by phishing emails, asking you to go to a bogus web site, open an attachment, reply to a criminal?

A. Yes

B. No

Criminal Methods and Techniques

- Smartphone Apps
  - Wall Street Journal: more than 50% take your personal info
  - No platform is entirely safe, even Apple's

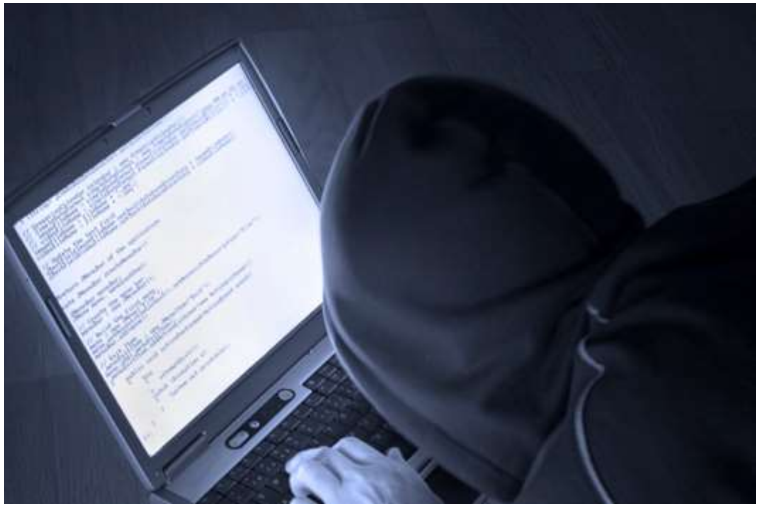
- Social Media Sites
  - Great for research – by criminals!
  - Be careful what you post!

Criminal Methods and Techniques

- Wireless Networks
  - A hacker's paradise if not secured
  - If not secured, DO NOT USE IT!
  - Even if it is, be very careful

The Most EFFECTIVE Technique

- Social Engineering
  - "psychological manipulation of people into performing actions or divulging confidential information" (Wikipedia)
  - The MOST effective tool
  - How Snowden did it
  - Scenarios
    - Market research
    - Remote help desk
    - Hacked email accounts



The Most EFFECTIVE Technique

- Social Engineering
- Beware the **wire transfer!**
  - Criminals do their research
  - They may register a domain name that has 1 character different from yours
  - Email comes from a principal to a finance employee requesting a wire transfer
  - This has worked MANY times!

Polling Question #4

How surprised are you by all this information?

A. Very surprised – I didn't know it was this bad.

B. Mildly surprised – I knew it was pretty bad.

C. Not surprised at all – I knew most of this.

Defending the Network

1. Job #1: Backups, Disaster Recovery, Business Continuity
   - Technology now offers many affordable solutions
   - Monitor the backups EVERY DAY!
   - Be sure to restrict access to the backups!
2. Physical Security: Lock the doors!
3. Password Policies
   - Require minimum length, complexity, and force changes
4. Layered security: Perimeter, network, files, applications
   - Firewalls with A/V, content filters, SSL deep packet inspection
   - Audit Network access rights
   - Audit File and Application access

Defending the Network

5. Monitor all network elements and access attempts
   - Alerts
   - Alarms
   - Logs

6. Third party penetration tests

7. Educate your fellow employees

8. Deploy Anti-Virus

Protect Yourself, Your Company, Our Nation

1. Change your passwords, make them strong, protect them
2. Report anything that is suspicious, and watch out for phishing
3. Never divulge any information to anyone you don’t know
4. Never use your work computer for personal use
5. Lock your computer: CTRL-ALT-DEL
6. Logoff your computer: Start – Shutdown – Logoff
7. Beware USB Flash Drives and Smart Phones
8. Never e-mail work products to your personal e-mail account
9. Stop using “free” music/video sharing sites
10. Download and configure Trusteer Rapport, the anti-key-logger from https://www.trusteer.com/ProtectYourMoney

Closing Thoughts

- Drive an organic thought process
- Set the tone ("Culture") and involve cross function teams
- Perform a risk assessment and identify / monitor metrics
- Keep an eye on 3rd party vendors
- Keep board and stakeholders informed on progress

Questions??

Thank You

Dan Gibson
Partner
EisnerAmper LLP
Daniel.Gibson@eisneramper.com

Jerry Ravi
Partner
EisnerAmper LLP
Jerry.ravi@eisneramper.com

Bill Blum
President
Alpine Business Systems
bblum@alpinebiz.com

EisnerAmper

This publication is intended to provide general information to our clients and friends, It does not constitute accounting, tax, or legal advice; nor is it intended to convey a thorough treatment of the subject matter.

EisnerAmper LLP
Accountants & Advisors

www.eisneramper.com

Appendix & Exhibits

EISNERAMPER

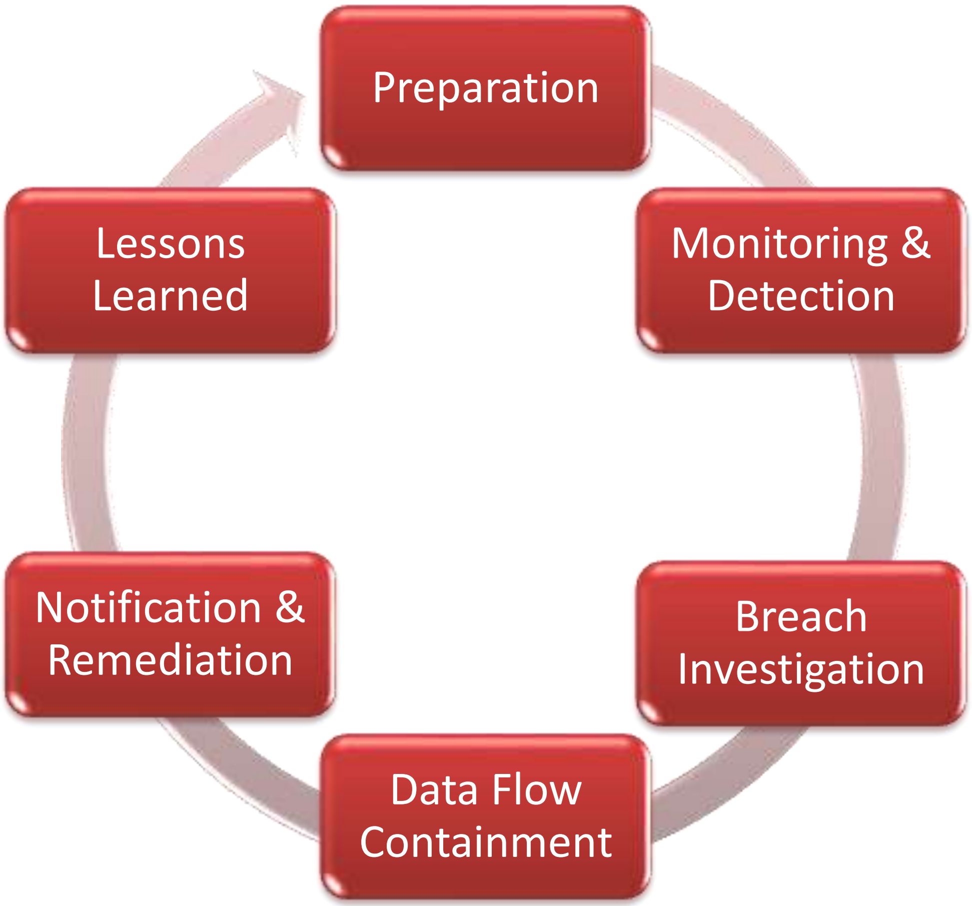
Defining the GAP: From the Board Room

- Board Members admit that their knowledge about cybersecurity is limited
- Board members and IT security professionals need to communicate on a regular basis
- IT security professionals are skeptical about their boards' understanding of cybersecurity risks
- Board members may be overly confident about the effectiveness of their cybersecurity governance practices
- It took the Target breach to get the board's attention

CYBERSECURITY & THE IMPORTANCE OF AN INFORMED BOARD MEMBER

Study conducted by Ponemon Institute, June 2015

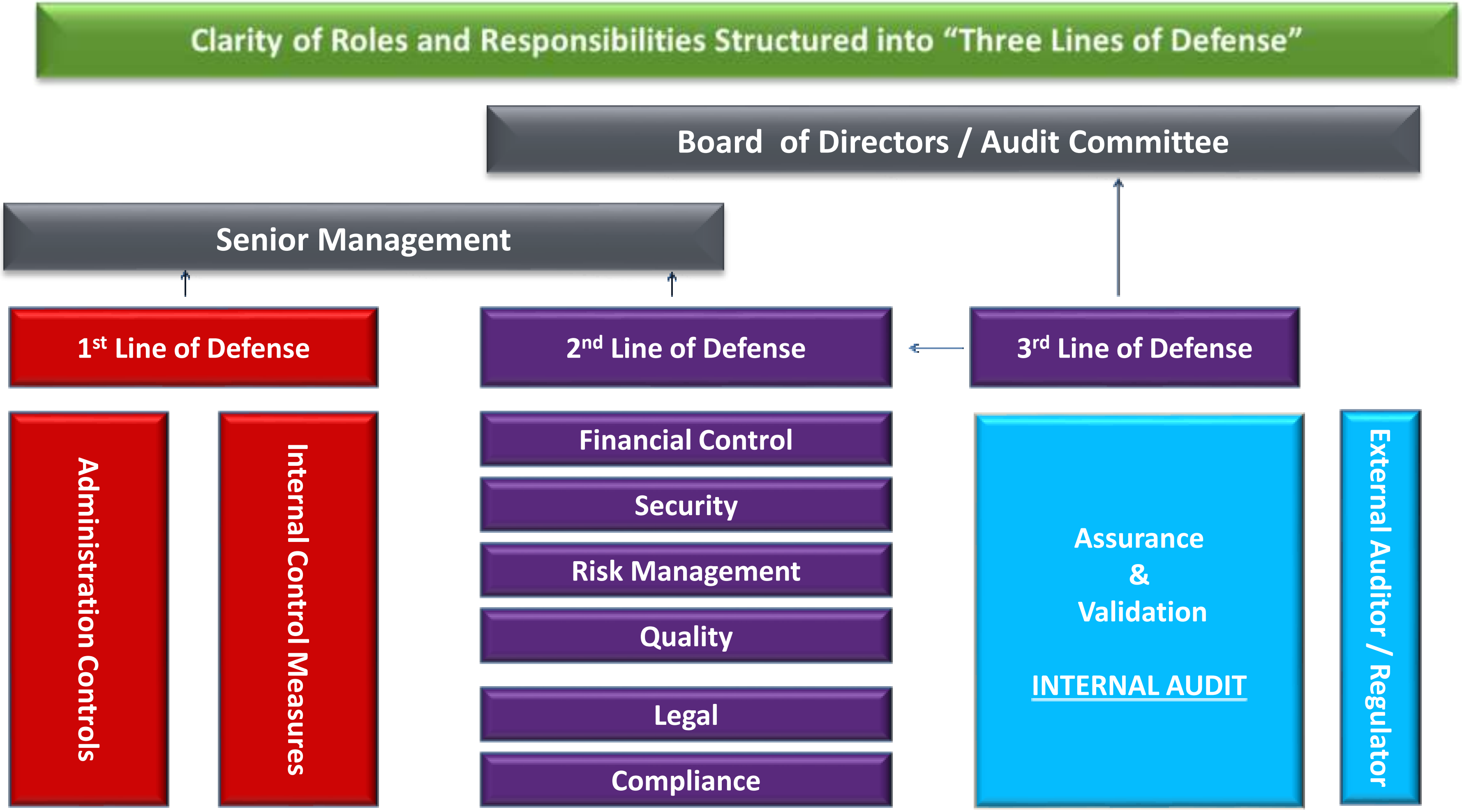
Incident Response Process Flow



* Program phases are based on SANS security incident handling model

- **Prep**:
  Process Definition, Data Classification, Table Top Exercise
- **Detect**:
  Receive Notification from Business Unit, IT
- **Investigate**:
  Determine if a Data Breach has Occurred
- **Contain**:
  Ensure that Data Leakage is Stopped
- **Remediate**:
  External Notifications & Remediation
- **Learn**:
  Varies with Incident

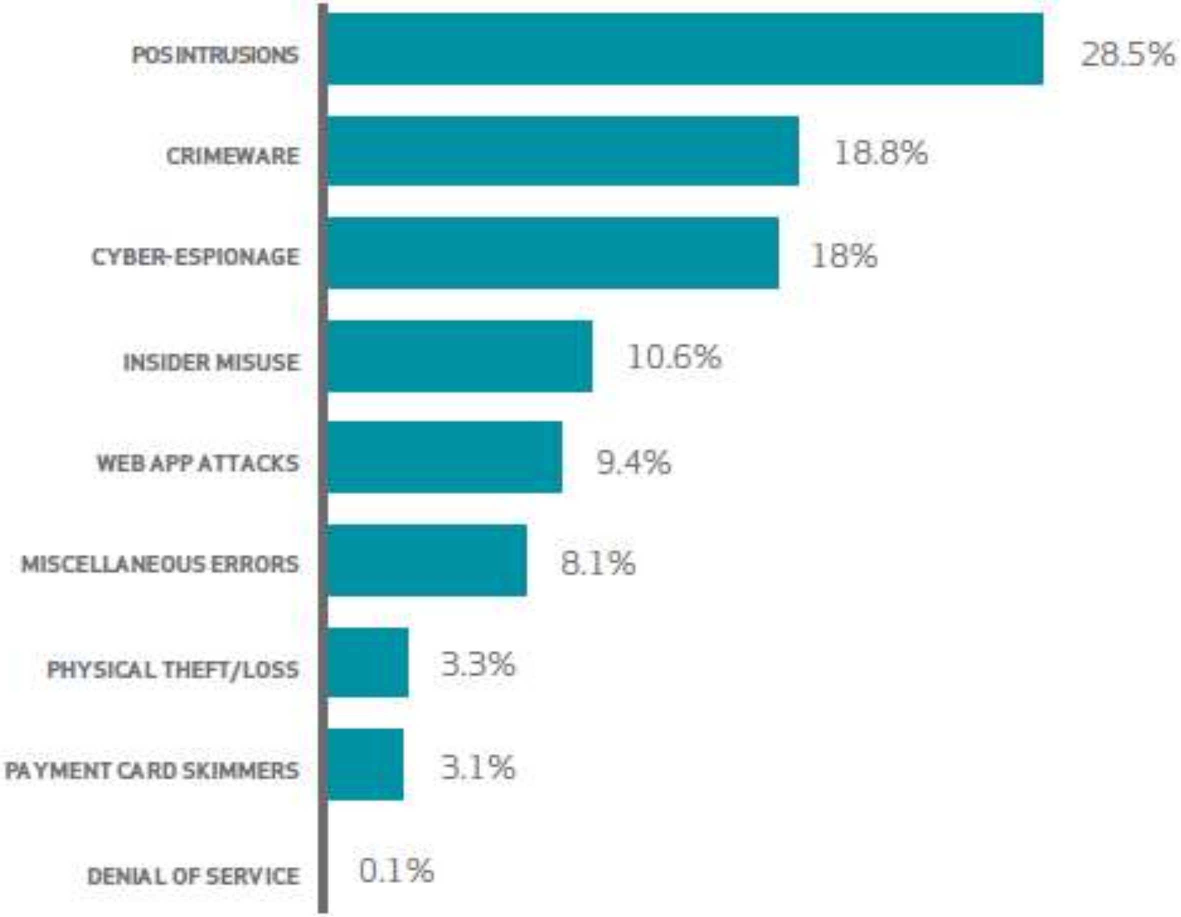
Three Lines of Defense Drives Governance Structure



EISNERAMPER

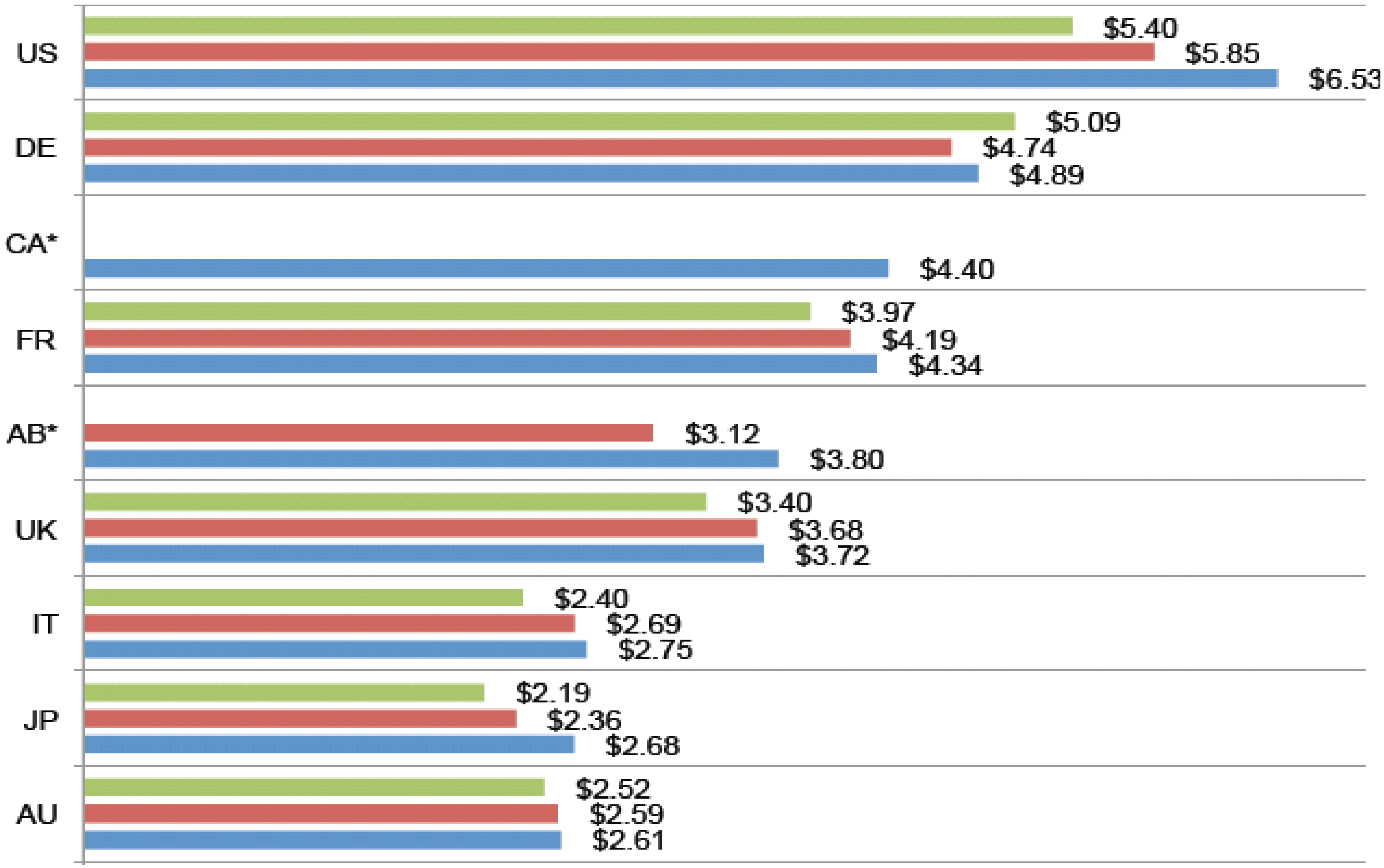
ALPINE BUSINESS SYSTEMS, INC.

General Frequency of Breach Type



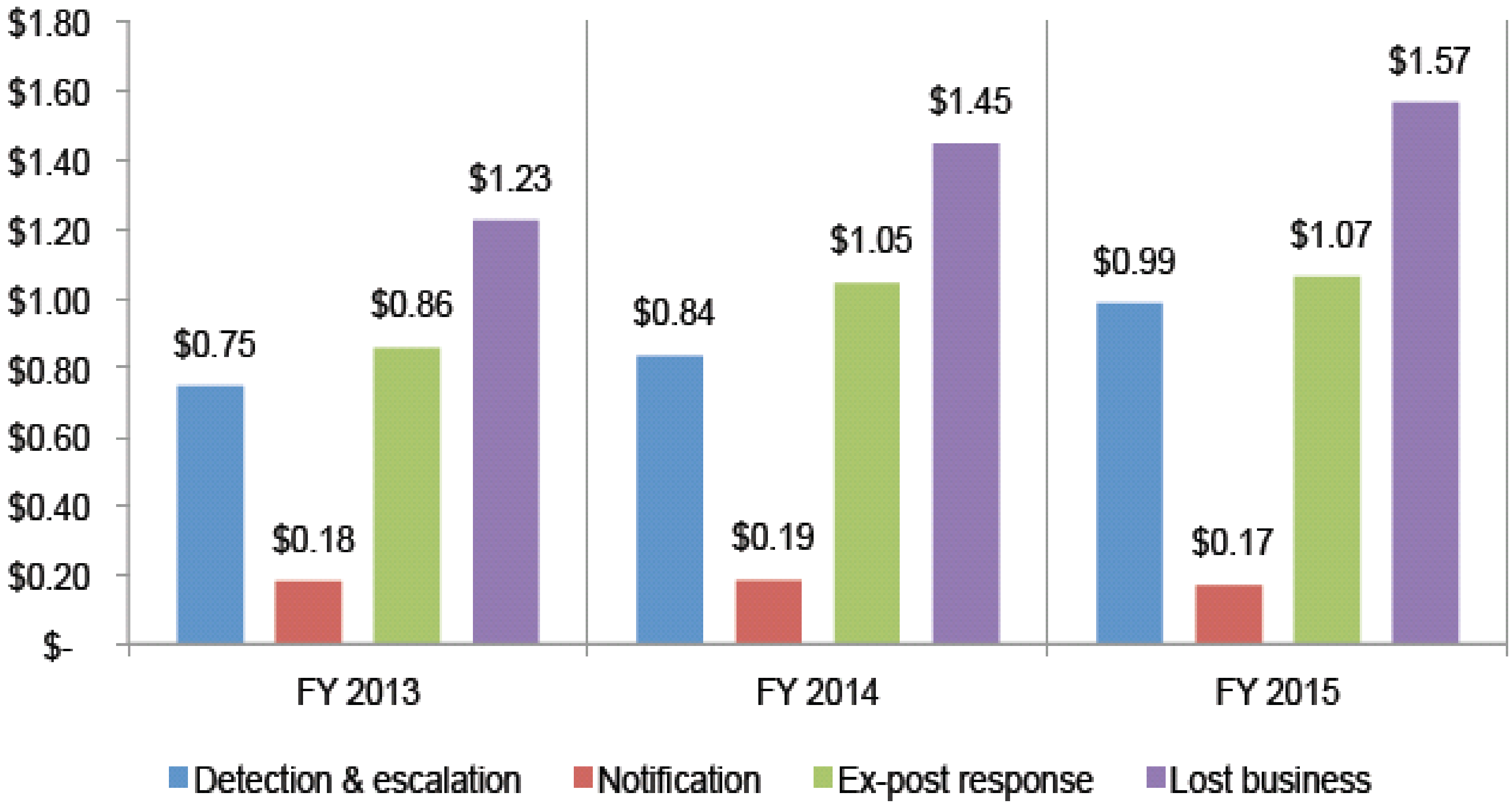
(Verizon, 2015 Data Breach Investigations Report)

Average Total Organizational Loss Resulting from a Data Breach



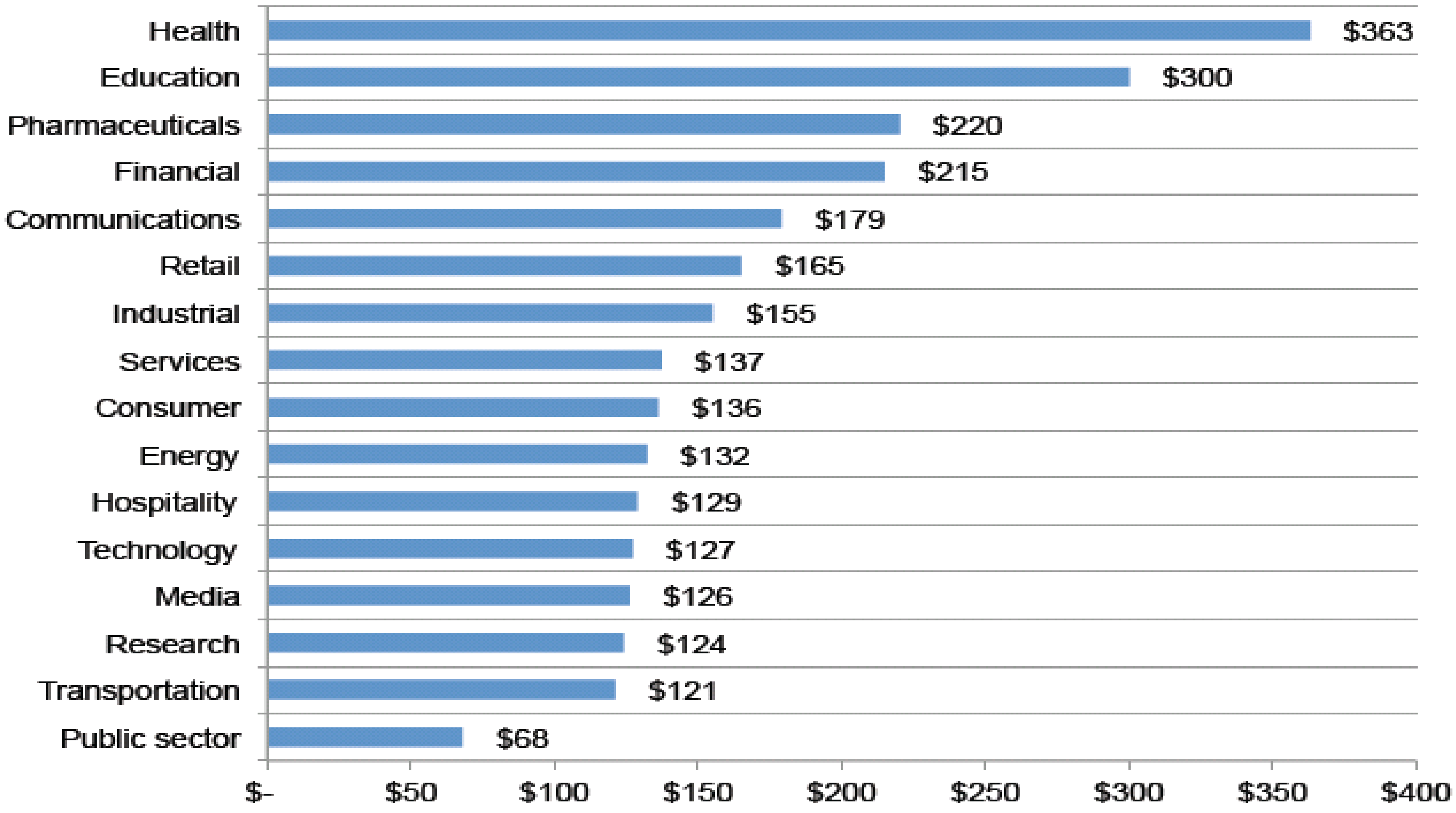
(Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis) US$ (millions)

Three Year Average: Data Breach Cost Components



(Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis) US$ (millions)

Average Remediation Cost per Victim by Industry



(Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis)