CYBER SECURE WORK INC

WHERE INFORMATION SECURITY, PRIVACY AND INSURANCE MEET.

National League of Cities

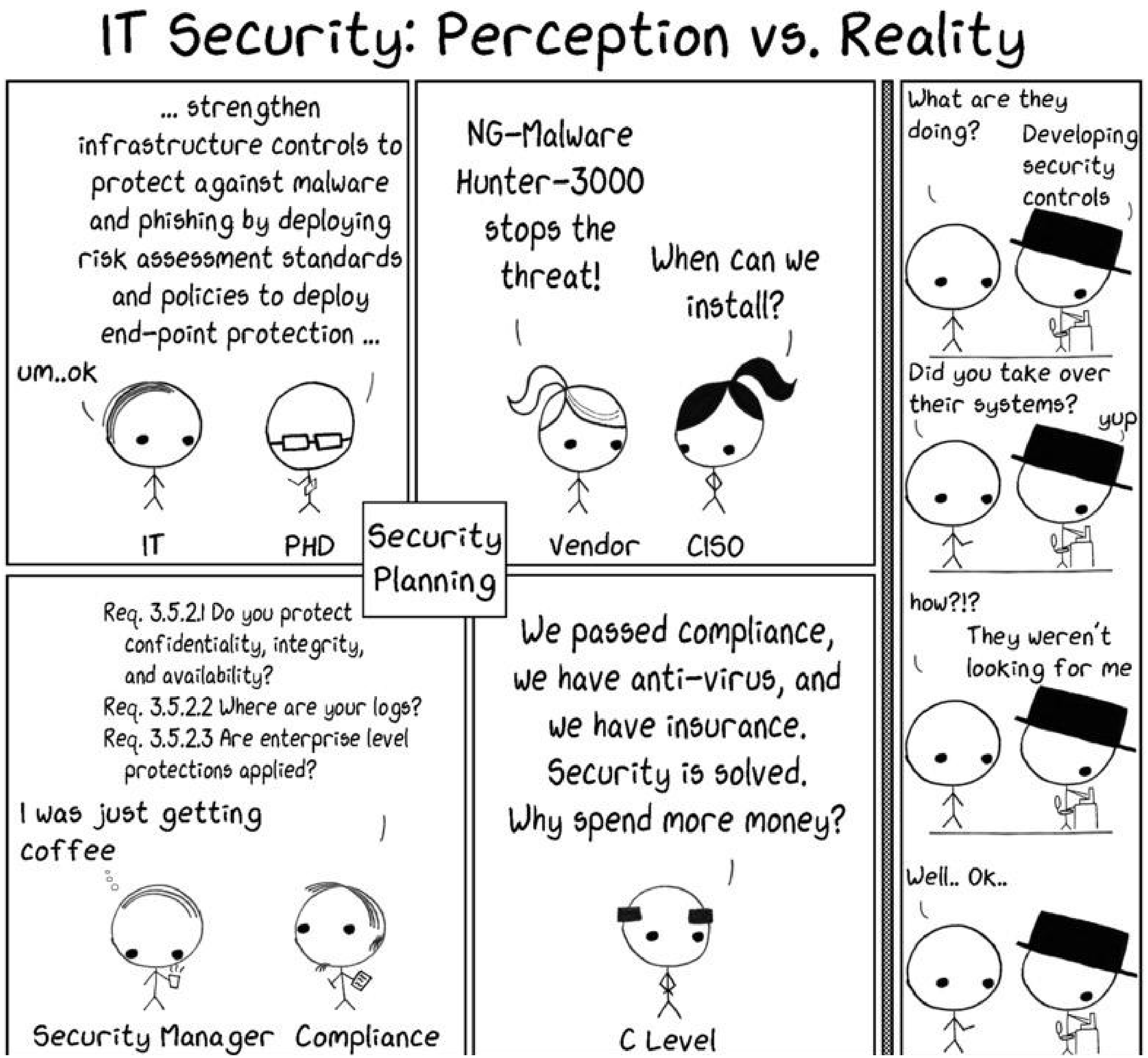
Risk Information Sharing Consortium

Libby Benet, JD , CIPP-US, CIPM
President, Cyber Secure Work, Inc.
October 16, 2019

“It’ll Never Happen to Me”: Avoiding and Managing Cyber Attacks On Municipalities

- Level Setting
- 15 Alarming Stats
- What Are The Threats?
- What Needs Protecting?
- Common Types of Attacks
- Frameworks/Standards/Compliance
- Compliance v. Security
- Systems Fail. Now What?
- Typical Types of Coverages and Services
- Issues to Growth

It's Complicated…


IT Security: Perception vs. Reality
… strengthen infrastructure controls to protect against malware and phishing by deploying risk assessment standards and policies to deploy end-point protection …
um..ok
IT
PHD
NG-Malware Hunter-3000 stops the threat!
When can we install?
Vendor
CISO
Security Planning
Req. 3.5.2.1 Do you protect confidentiality, integrity, and availability?
Req. 3.5.2.2 Where are your logs?
Req. 3.5.2.3 Are enterprise level protections applied?
I was just getting coffee
Security Manager
Compliance
We passed compliance, we have anti-virus, and we have insurance. Security is solved. Why spend more money?
C Level
What are they doing?
Developing security controls
Did you take over their systems?
yup
how?!?
They weren't looking for me
Well.. Ok..

What do Business Leaders Need To Know - Information Security

Objective of information security is to ensure information’s **confidentiality**, **integrity, availability** and **accountability**.

The focus of information security is **to reduce** the potential for **damage** to, **loss** of, **modification** of or **unauthorized access** to systems, facilities or data.

Information security includes the **technical** and **physical controls of IT systems**, **building security, remote users, vendors, third parties** and the **creation and maintenance of business-continuity** and **disaster-recovery plans**.

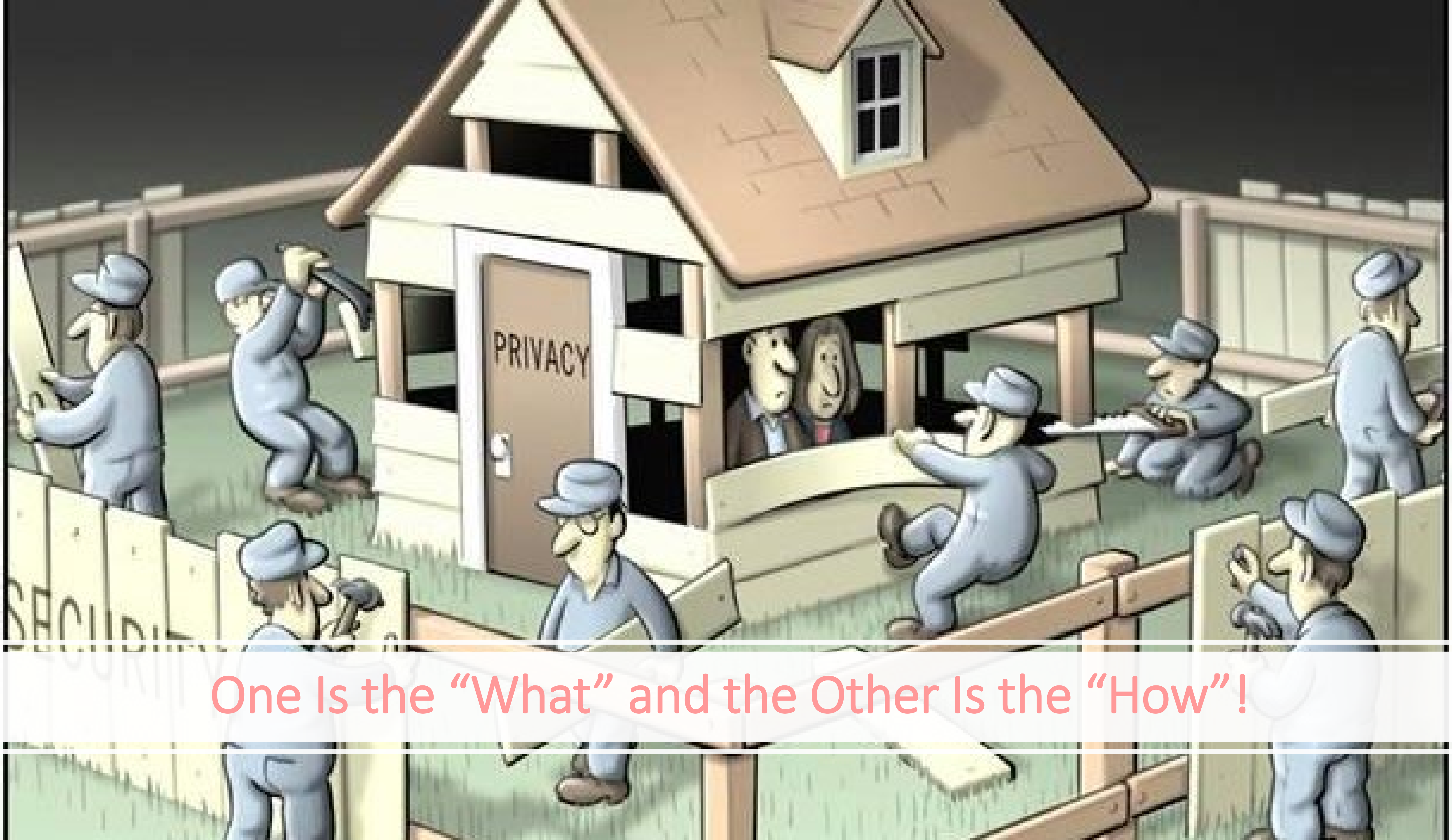
What do Business Leaders Need To Know - Privacy

The objective of **privacy protections** is to ensure that individuals receives the following considerations about their protected data:

Notice, choice and consent and the option to correct misinformation

Privacy protections attach to the people who give a business their personal information.

These protections are concerned with **the individual's ability to control** the use of that information.



One Is the “What” and the Other Is the “How”!

15 Alarming Cyber Security Facts and Stats According to Cybint Solutions:

- 95% of breached records came from only three industries in 2016
- There is a hacker attack every **39 seconds**
- **43% of cyber attacks target small business**
- The **average cost** of a data breach in 2020 **will exceed $150 million**
- In 2018 hackers **stole half a billion personal records**
- Over **75% of healthcare industry has been infected** with malware over last year
- **Large-scale DDoS attacks increase in size by 500%**

https://www.cybintsolutions.com/cyber-security-facts-stats/

15 Alarming Cyber Security Facts and Stats According to Cybint Solutions:

- Approximately **$6 trillion** is expected **to be spent globally** on cybersecurity by 2021
- By **2020** there will be roughly **200 billion connected devices**
- **Unfilled** cybersecurity jobs worldwide will reach **3.5 million by 2021**
- **95%** of cybersecurity breaches are due to **human error**
- More than **77%** of organizations **do not have a Cyber Security Incident Response plan**
- Most companies **take nearly 6 months to detect** a data breach, even major ones
- 46% of all Bitcoin transactions involve illegal online activity
- Total cost for cybercrime committed globally has added up to over $1 trillion dollars in 2018

https://www.cybintsolutions.com/cyber-security-facts-stats/

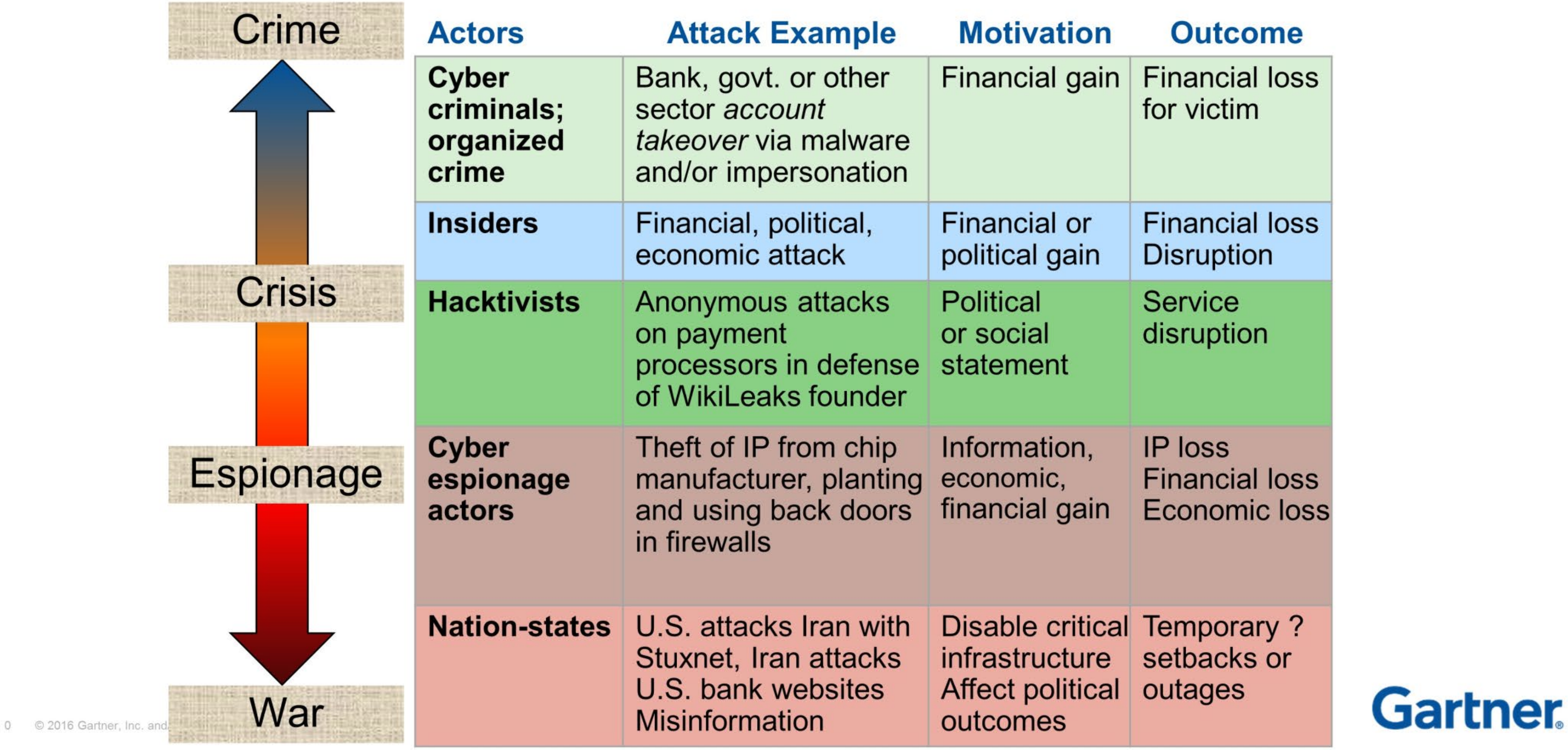
Where Are the Insider Threats?

- Employee negligence
  - Security failures
  - Lost portable devices
  - Unintended disclosures by email, fax, phone or in person
- Failure to encrypt portable devices
- Employee ignorance
  - Improper disposal of personal information (dumpsters)
  - Lack of education and awareness
- Malicious and/or nosey employees

Where Are the Outside Threats?

- Hackers
  - Malware
  - Phishing and spear phishing
- Thieves/Organized Crime
  - Social engineering tools
  - Stolen portable devices
- Vendors/Business Associates
- Nation State Actors

Where Is the Risk? Threat Actors and Their Attacks



Crime

Crisis

Espionage

War

Actors	Attack Example	Motivation	Outcome
Cyber criminals; organized crime	Bank, govt. or other sector *account takeover* via malware and/or impersonation	Financial gain	Financial loss for victim
Insiders	Financial, political, economic attack	Financial or political gain	Financial loss Disruption
Hacktivists	Anonymous attacks on payment processors in defense of WikiLeaks founder	Political or social statement	Service disruption
Cyber espionage actors	Theft of IP from chip manufacturer, planting and using back doors in firewalls	Information, economic, financial gain	IP loss Financial loss Economic loss
Nation-states	U.S. attacks Iran with Stuxnet, Iran attacks U.S. bank websites Misinformation	Disable critical infrastructure Affect political outcomes	Temporary ? setbacks or outages

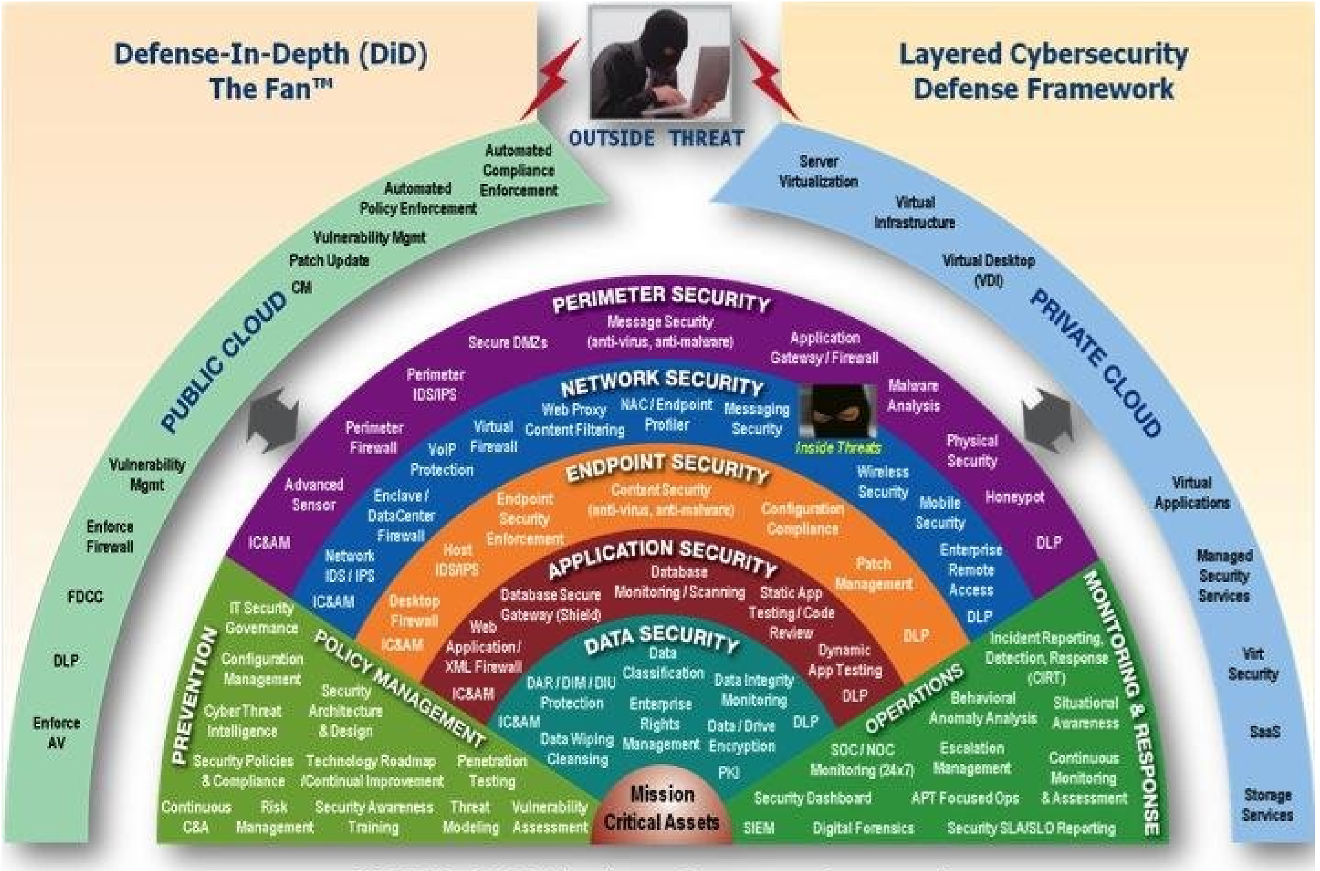
Gartner

The Landscape To Secure

- Desktops
- Laptops
- Networks
- Mobile
- Websites
- Email
- Industrial Control Devices
- Cloud
- Internet of Things (IoT)

What Does It Mean To Protect?
Defense In Depth

- https://www.researchgate.net/figure/The-Fan-illustrating-technology-and-process-defense-in-depth-architectural-pictorial_fig1_278676540



© 2010, 2012 Northrop Grumman Corporation

What data is there to protect?

- Mortgage documents, deeds, births, deaths, ugly divorces, medical records, Social Security numbers and military discharge documents are among the many types of publicly accessible documents that may contain PII (personally identifiable information), PHI (personal health information) or other sensitive data.

https://www.cio.com/article/3184618/county-and-municipal-cybersecurity-part-1.html

What Is Happening? - City of Baltimore

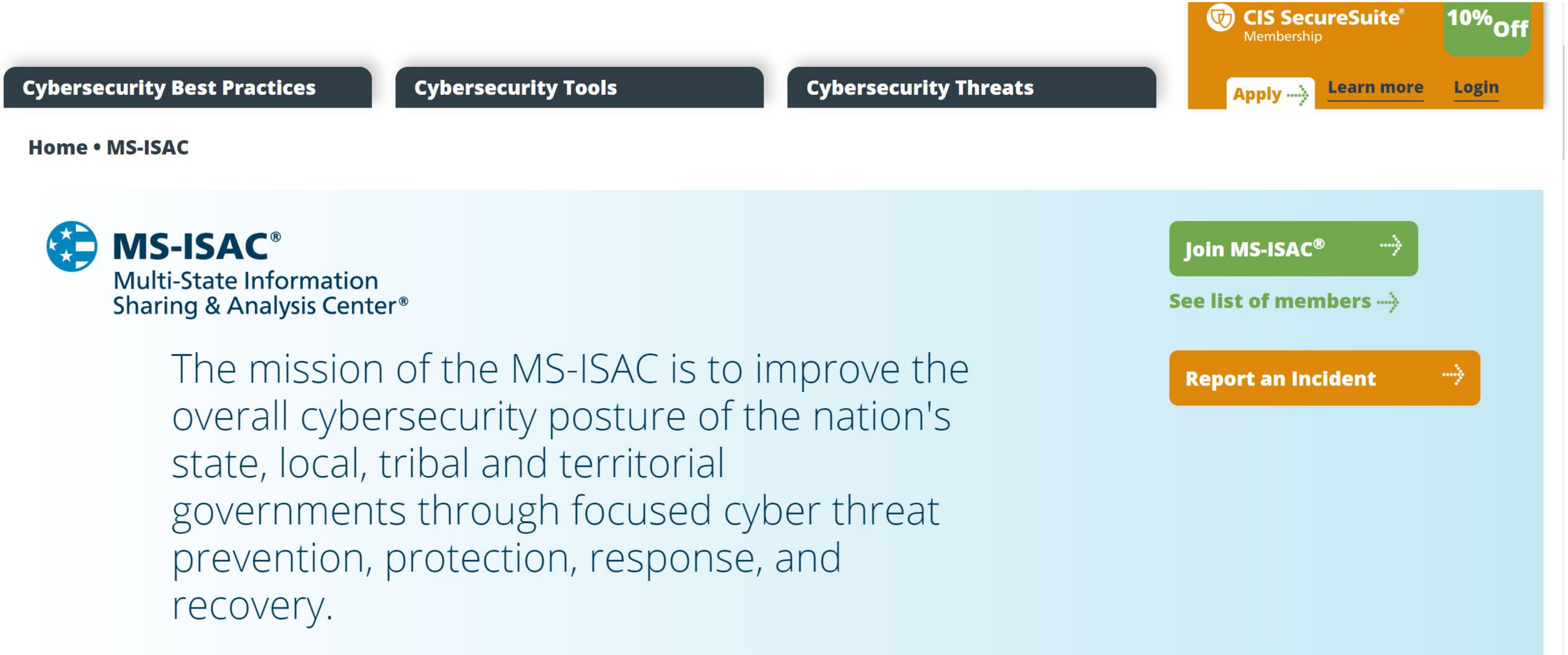
https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html

2019 Events….

According to CNN, "Just this year alone, 140 attacks targeting public state and local governments and health care providers have been reported, according to a tally by the cybersecurity firm Recorded Future, which has tracked attacks on local governments since 2013 and the healthcare industry since 2016."

https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html

Center For Internet Security



The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

https://www.cisecurity.org/ms-isac/

5 Top Security Concerns of the Center For Internet Security

- Lack of funding for cyber
- Inadequate cyber professionals
- Increasing sophistication of threats
- Lack of documented practices
- Emerging technologies

Issues for Municipalities

- Lack of skilled and trained personnel in cybersecurity.
- Lack of disaster recovery plans.
- Lack of third-party risk management in place for their supply chain.
- Complexity of state and federal regulations. (e.g. HIPPA, Mental Health Regulations, Criminal Justice Regs, Department of Health).
- Shared Infrastructure.
- Decentralized/Siloed management of IT/IS.
- Budget limitations.
- Lack of cybersecurity training for employees.

https://www.pivotpointsecurity.com/blog/local-government-cyber-security-issues/

Common Types of Cyber Attacks

Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms.

Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

Once inside the system, malware can do the following:

- Blocks access to key components of the network (ransomware)
- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Common Types of Cyber Attacks

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.

The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.

Phishing is an increasingly common cyberthreat.

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Common Types of Cyber Attacks

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.

2. Once malware has breached a device, an attacker can install software to process all of the victim's information.

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Common Types of Cyber Attacks

A **denial-of-service attack** floods systems, servers, or networks with traffic to exhaust resources and bandwidth.

As a result, the system is unable to fulfill legitimate requests.

Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Common Types of Cyber Attacks

A **Structured Query Language (SQL)** injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.

An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Common Types of Cyber Attacks

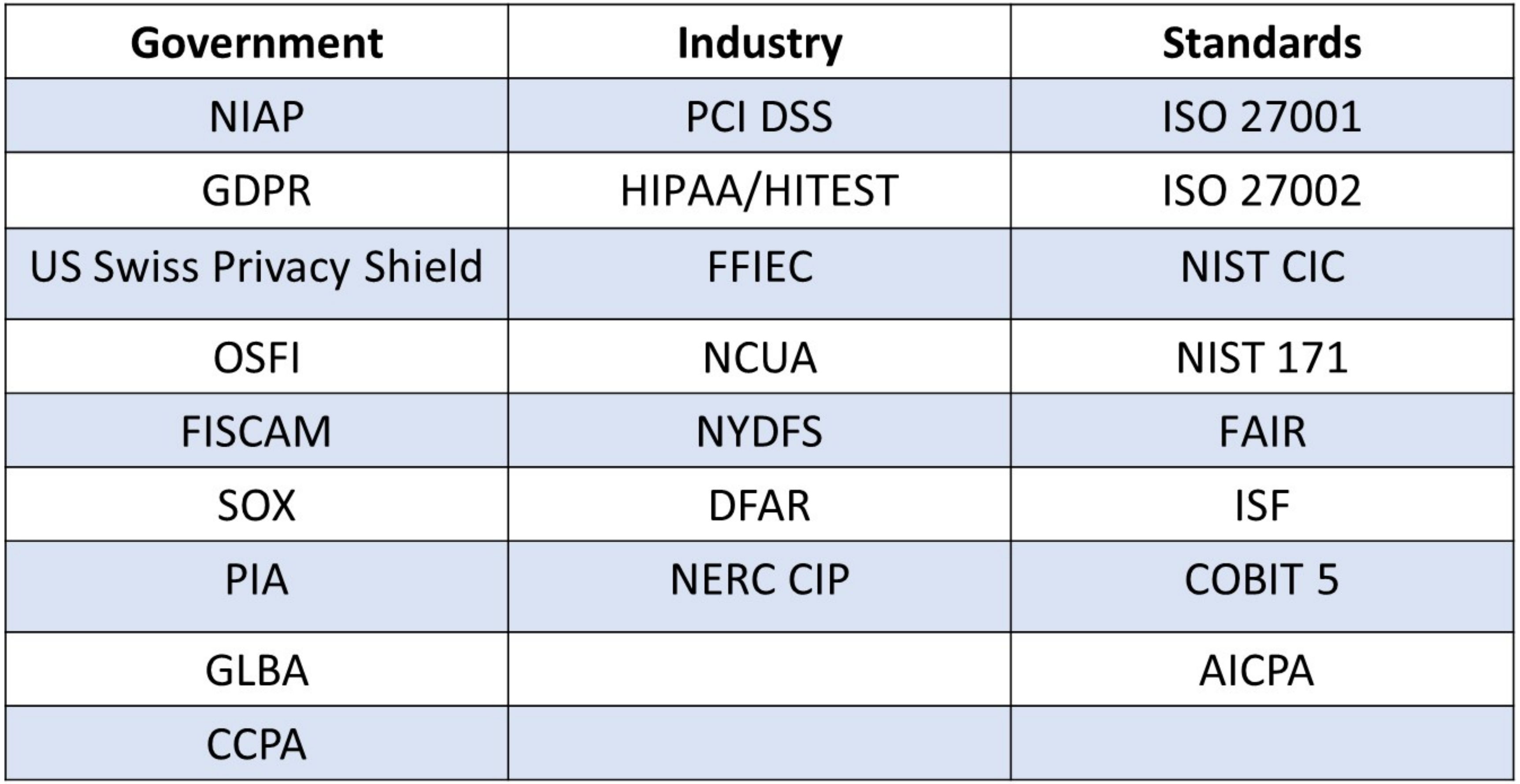
A **zero-day exploit** hits after a network vulnerability is announced but before a patch or solution is implemented.

Attackers target the disclosed vulnerability during this window of time.

Zero-day vulnerability threat detection requires constant awareness.

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Frameworks/Standards/Compliance



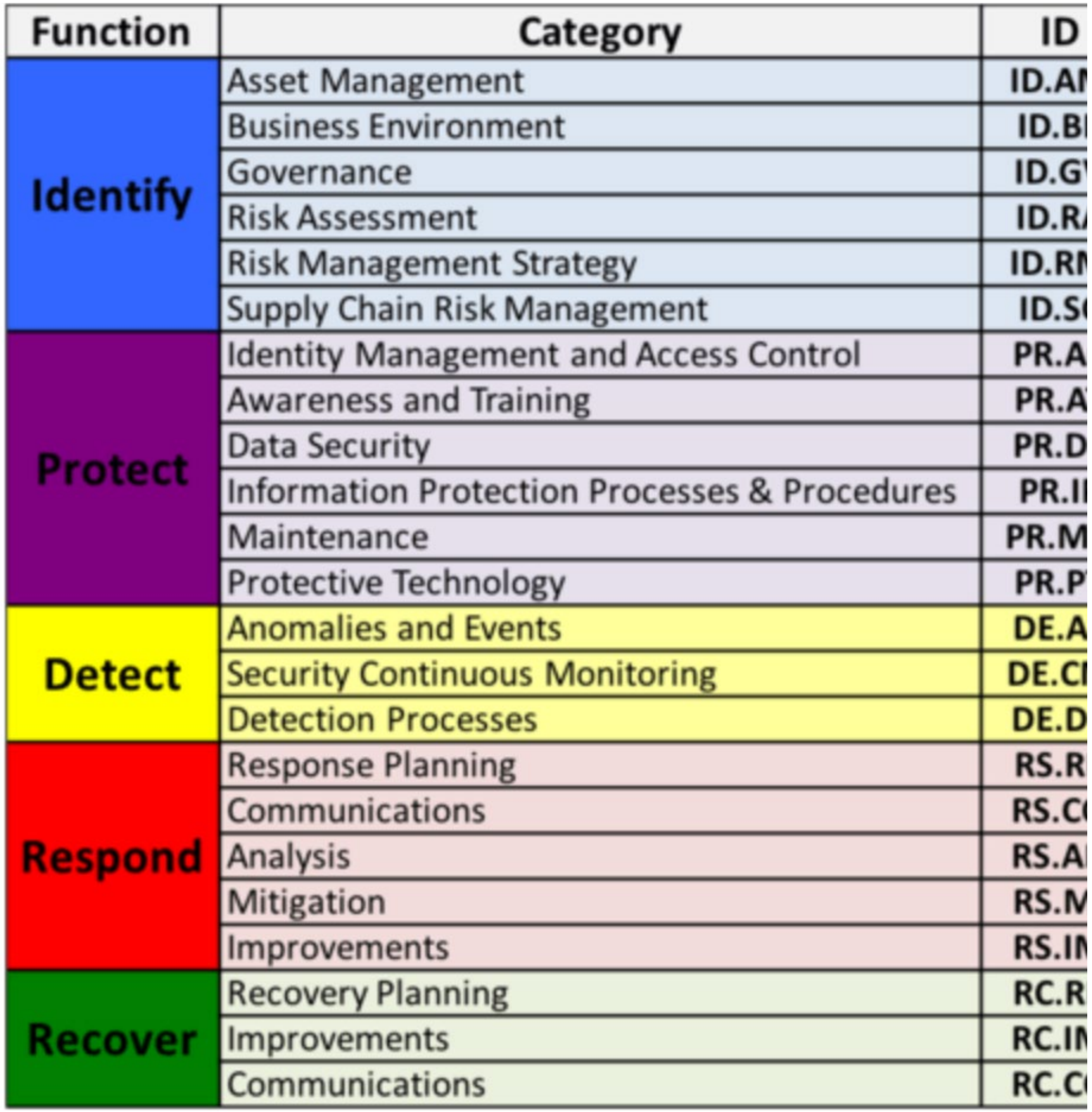
Government	Industry	Standards
NIAP	PCI DSS	ISO 27001
GDPR	HIPAA/HITEST	ISO 27002
US Swiss Privacy Shield	FFIEC	NIST CIC
OSFI	NCUA	NIST 171
FISCAM	NYDFS	FAIR
SOX	DFAR	ISF
PIA	NERC CIP	COBIT 5
GLBA		AICPA
CCPA		

Key Areas Covered in Assessments

- ACCEPTABLE USE/EMPLOYEE DATA POLICY
- IDENTITY AND ACCESS POLICY
- BUSINESS-CONTINUITY PLANNING/DISASTER-RECOVERY PLAN EXECUTION
- DATA CLASSIFICATION AND PRIVACY
- INCIDENT MANAGEMENT
- VULNERABILITY SCANS/PENETRATION TESTING
- COMPANY CULTURE/GOVERNANCE
- ACTUAL BREACH/CYBER HAZARD EVENT

NIST Framework

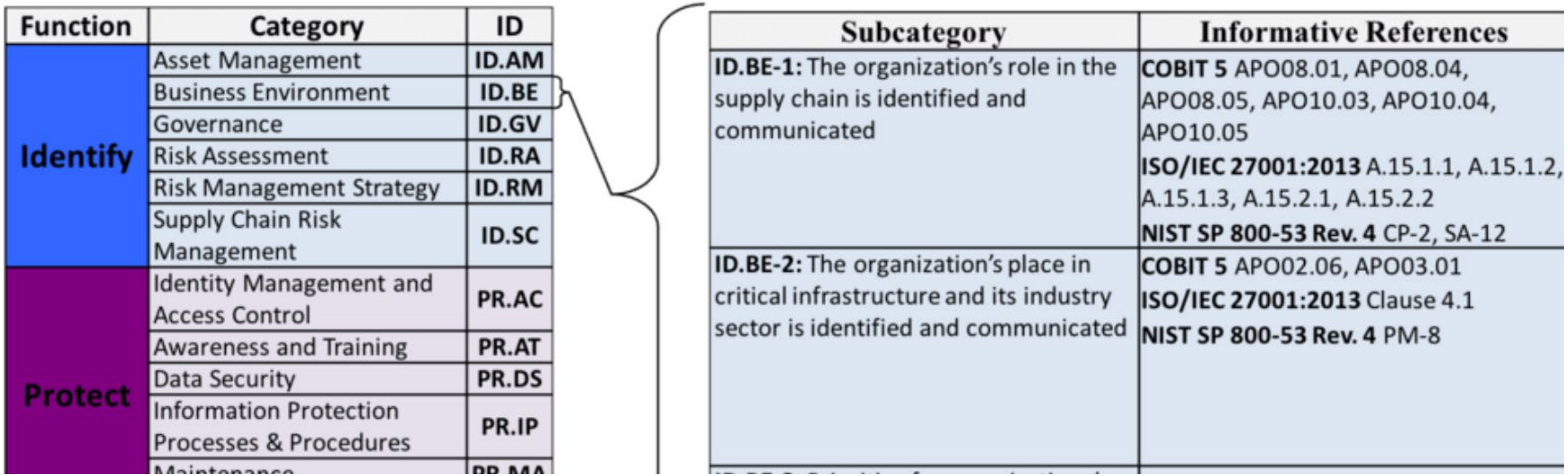
“Because the Framework is outcome driven and **does not mandate how an organization must achieve those outcomes**, it enables risk-based implementations that are customized to the organization's needs. “



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.B
	Governance	ID.G
	Risk Assessment	ID.R
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.S
Protect	Identity Management and Access Control	PR.A
	Awareness and Training	PR.A
	Data Security	PR.D
	Information Protection Processes & Procedures	PR.I
	Maintenance	PR.M
	Protective Technology	PR.P
Detect	Anomalies and Events	DE.A
	Security Continuous Monitoring	DE.C
	Detection Processes	DE.D
Respond	Response Planning	RS.R
	Communications	RS.C
	Analysis	RS.A
	Mitigation	RS.M
	Improvements	RS.IM
Recover	Recovery Planning	RC.R
	Improvements	RC.IM
	Communications	RC.C

National Institute of Science and Technology Cybersecurity Framework Core

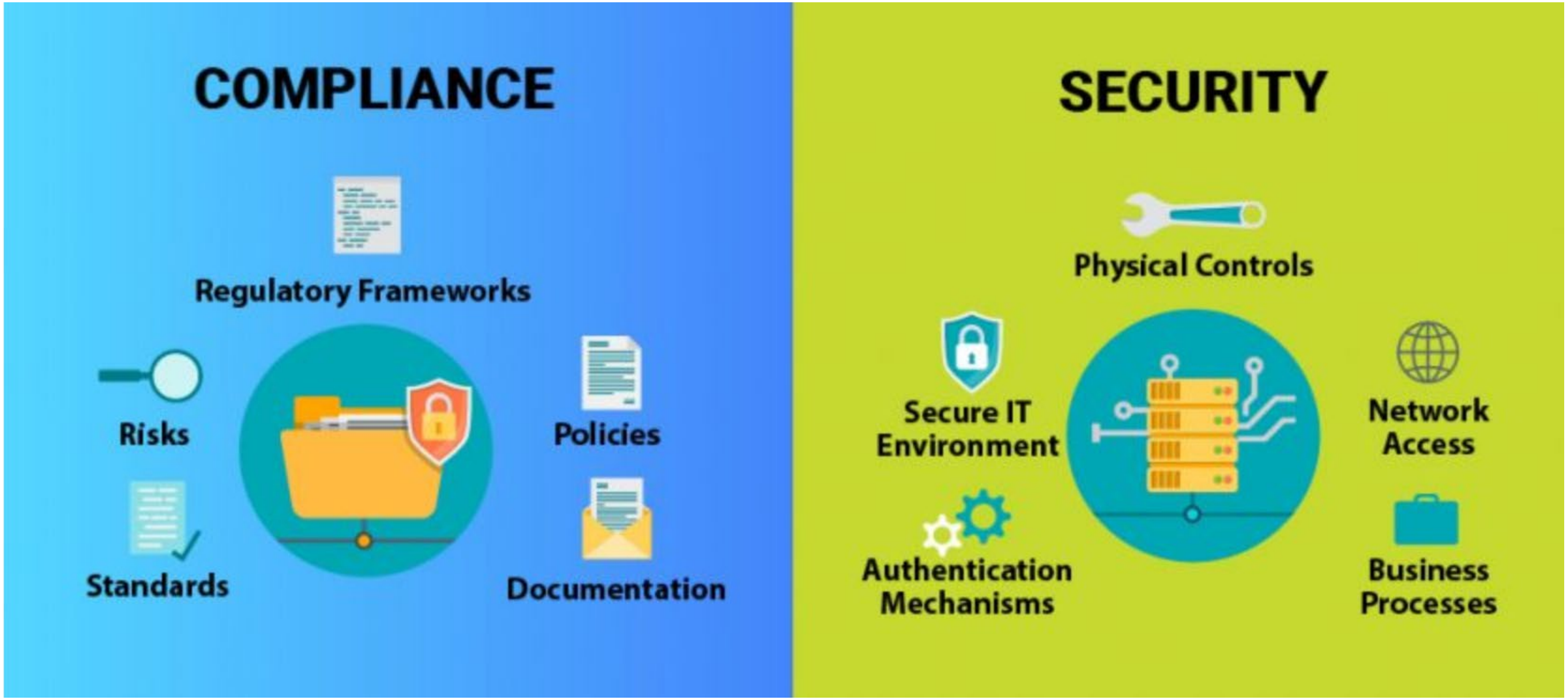
Deeper Dive



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA

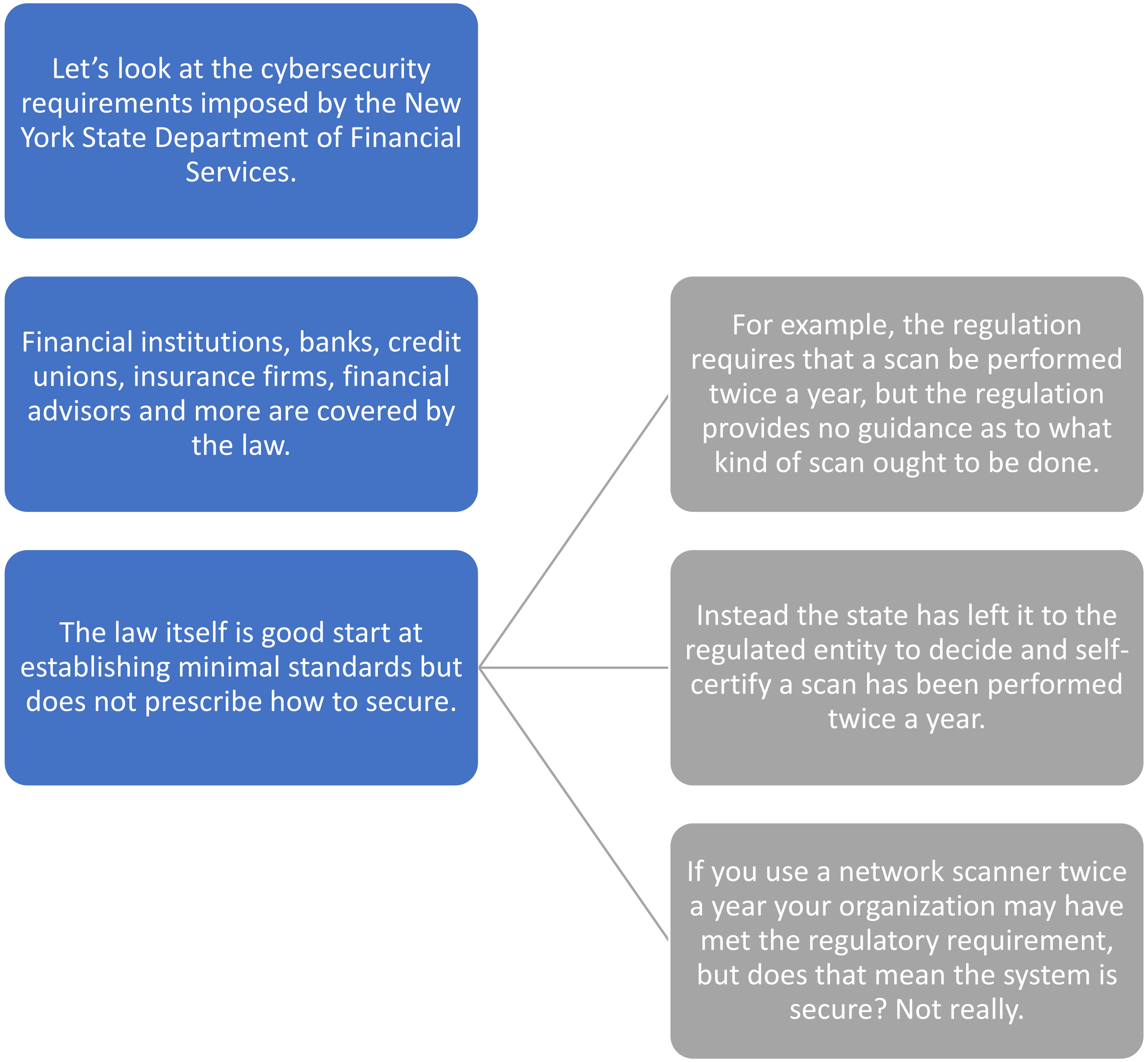
Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8

Compliance v. Security - What's the difference?



https://phoenixnap.com/blog/security-vs-compliance

Compliance v. Security



Let’s look at the cybersecurity requirements imposed by the New York State Department of Financial Services.

Financial institutions, banks, credit unions, insurance firms, financial advisors and more are covered by the law.

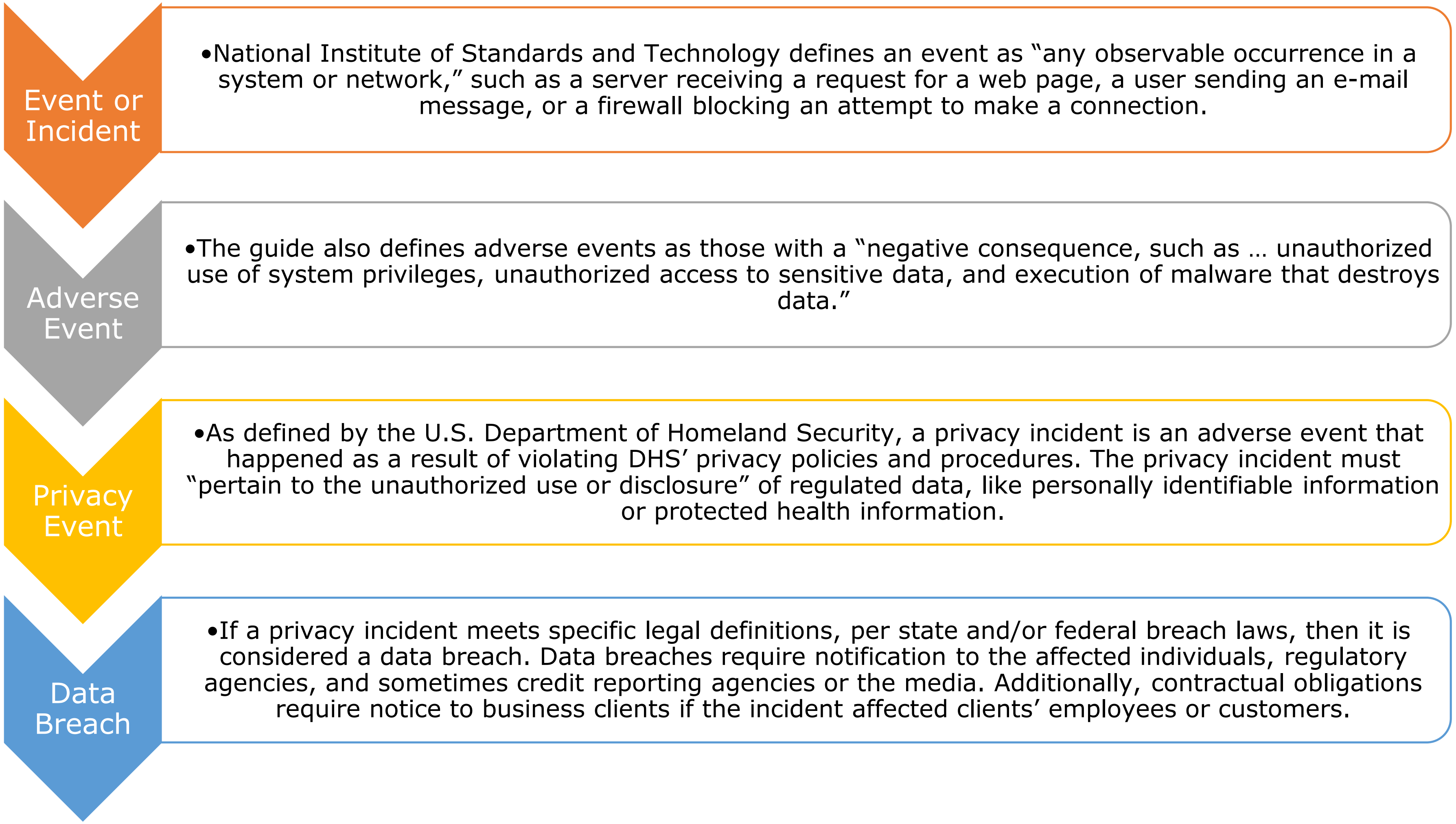
The law itself is good start at establishing minimal standards but does not prescribe how to secure.

For example, the regulation requires that a scan be performed twice a year, but the regulation provides no guidance as to what kind of scan ought to be done.

Instead the state has left it to the regulated entity to decide and self-certify a scan has been performed twice a year.

If you use a network scanner twice a year your organization may have met the regulatory requirement, but does that mean the system is secure? Not really.

You did all the right things, but the system failed anyway. Now what?



Event or Incident

- National Institute of Standards and Technology defines an event as "any observable occurrence in a system or network," such as a server receiving a request for a web page, a user sending an e-mail message, or a firewall blocking an attempt to make a connection.

Adverse Event

- The guide also defines adverse events as those with a "negative consequence, such as … unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data."

Privacy Event

- As defined by the U.S. Department of Homeland Security, a privacy incident is an adverse event that happened as a result of violating DHS' privacy policies and procedures. The privacy incident must "pertain to the unauthorized use or disclosure" of regulated data, like personally identifiable information or protected health information.

Data Breach

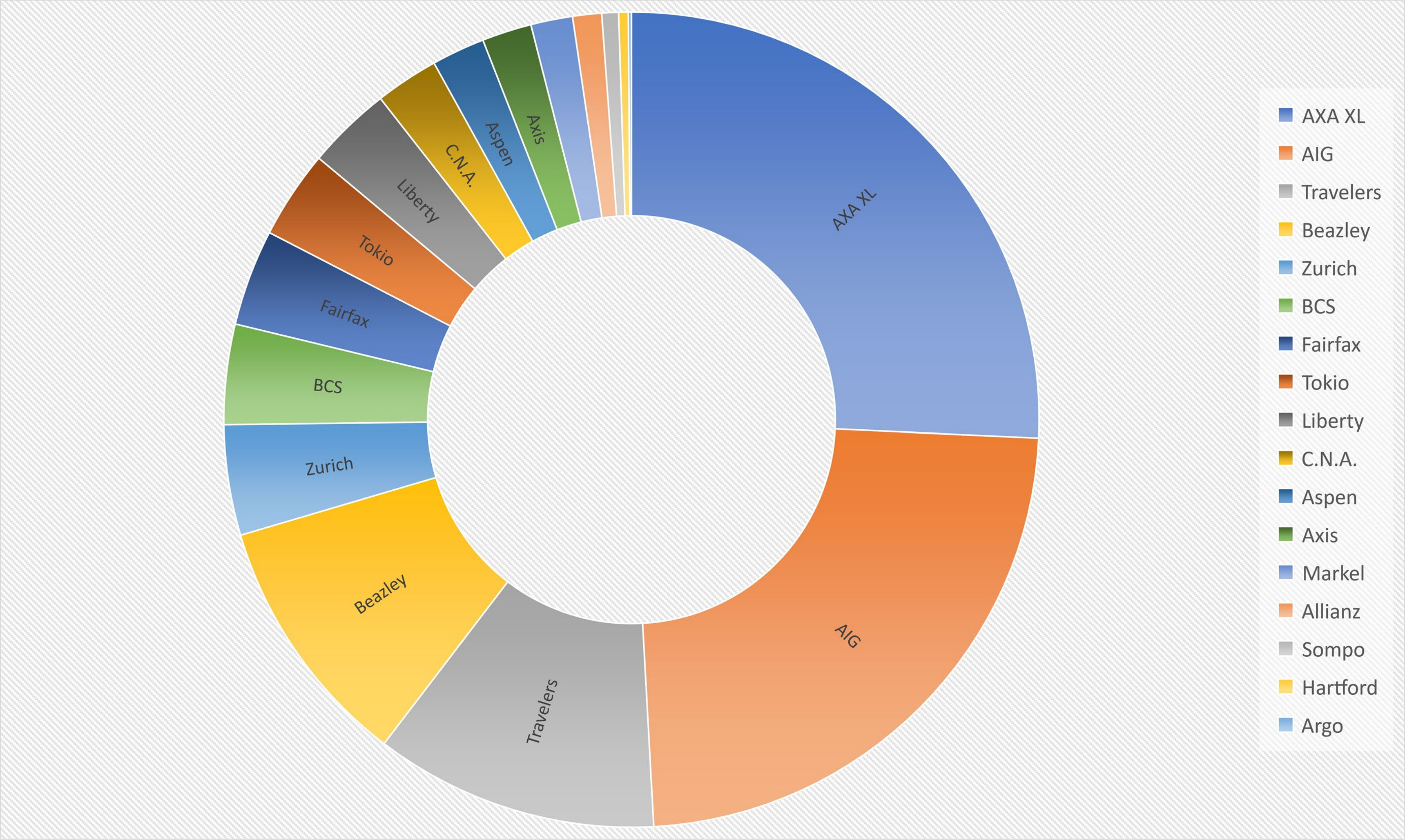
- If a privacy incident meets specific legal definitions, per state and/or federal breach laws, then it is considered a data breach. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies or the media. Additionally, contractual obligations require notice to business clients if the incident affected clients' employees or customers.

Is it an incident or a breach? How to tell and why it matters. https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/

Where Can the Losses Come From?

- Data breaches—personal data, corporate intellectual property compromised
- Malware/hostage for ransom
- Systems development/network security of the enterprise
- Digital supply chain
- Phishing/email and mobile phone text scams
- Regulatory fines—GDPR/California Consumer Data Privacy Act
- Business interruption, data restoration and data protection
- Liability for actual damages and punitive awards
- Bank recovery of card fraud loss
- Loss of funds/property through social engineering

US Insurance Industry – Stand Alone = $1B



Typical Types of Coverage and Services

Breach Response Services

- Privacy Council
- Forensics
- Credit Monitoring
- Public Relations & Crisis Management
- Required Notifications
- Voluntary Notifications
- Call Center
- Law firm to determine indemnification under contract with indep contractor
- Data Breach Coach
- Fraud Consultation to customers
- Restoration of Identity

Typical Types of Coverage and Services

First Party

- Business Interruption
- Systems Failure
- Consequential Reputational Income Loss
- Contingent Business Interruption
- Dependent Systems Failure
- Dependent Security Breach
- Cloud Computing
- Extortion
- Data Recovery
- Good Faith Advertising to regain customer loyalty

Typical Types of Coverage and Services

Third Party

- Network Liability
- Privacy Liability
- Regulatory Defense and Penalty
- Consumer Redress Fund
- Credit Card Liabilities and Costs
- Media Liability
- Miscellaneous Professional

Typical Types of Coverage and Services

Crime Coverages

- Fraudulent Instruction
- Funds Transfer Fraud
- Telephone Fraud
- Criminal Reward

Typical Types of Coverage and Services

- Employee Training
- Sample Incident Response Plans
- Educational pieces, posters, webinars
- Ala carte Prevention Services

Key Exclusions

Liability

- Bodily Injury and Property Damage
- Intentional or Criminal Acts
- War – is there a terrorism or nation state carve back?
- Loss of Funds

First Party

- Hardware or software replacement
- Fire, Flood, Earthquake etc

Prior Notice and Prior or Pending Litigation

Other Considerations

- Trigger - Claims Made for Liability
- Trigger - Incident Discovered for First Party
- Are Expenses Inside or Outside the Limit?
- Review Definitions
- How much Limit is Needed?
- Underwriting Process

On the Horizon

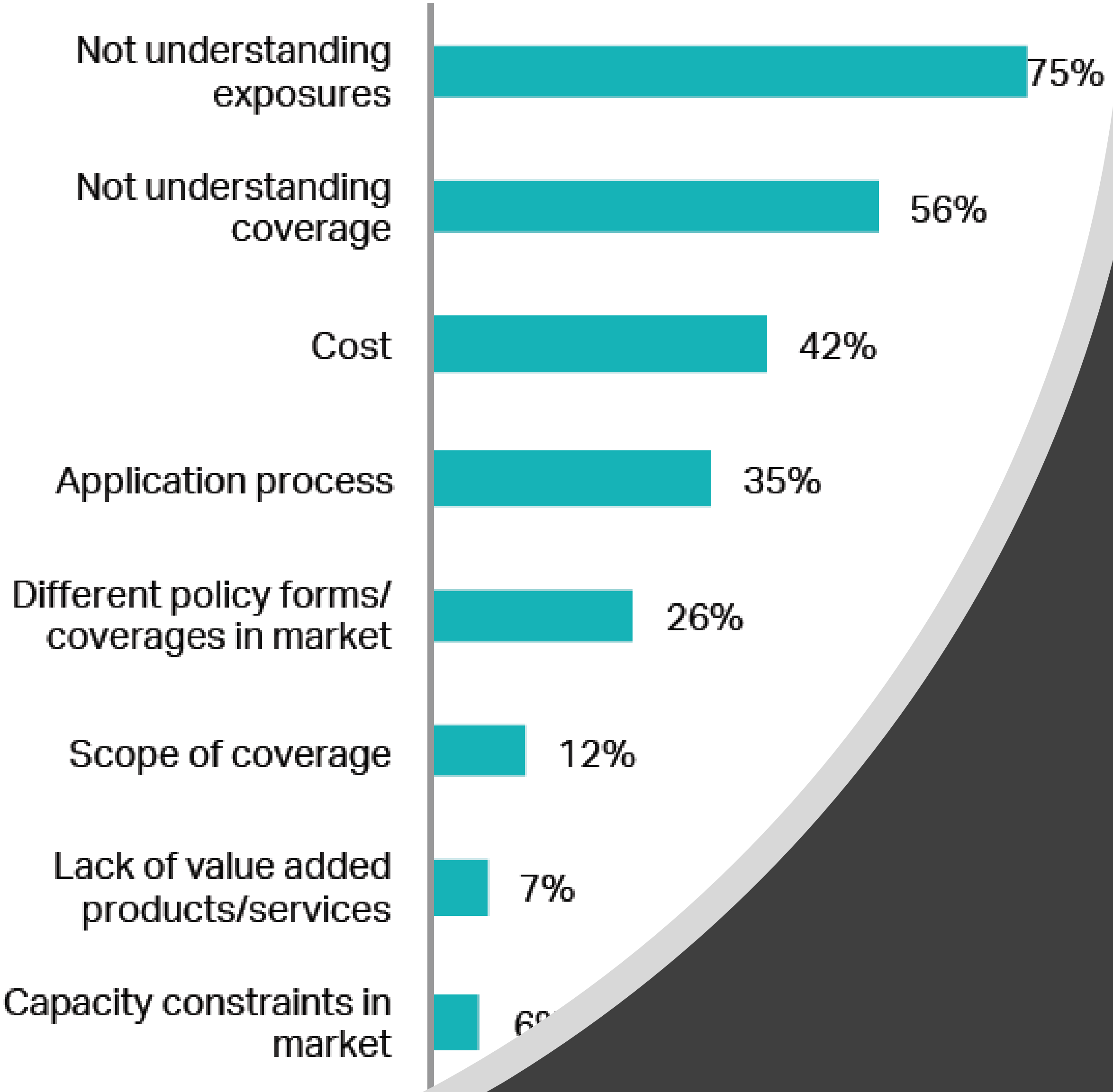
NEW PRIVACY LAWS – STATE OR FEDERAL

UN CYBERSECURITY GOVERNANCE

NEW TECHNOLOGIES

CYBER CAT

Q What are the biggest obstacles to writing cyber insurance policies? (select up to 3)



INDUSTRY ISSUES TO GROWTH

Advisen and Partner Re 2018 Survey

Of Cyber Insurance Market Trends

Thank you!

Any questions?