

Security - Relationships

- Security Strategy and Information Sharing

- Peter Allor
- Senior Security Strategist,
Project Manager, Disclosures
- IBM Security

- May 20, 2016



Paradigm shift in crime



Jason Corbin
Vice President
Offering Management and Strategy
Security Operations and Response



New technologies introduce new risks...

44%



of security leaders expect a major cloud provider to suffer a security breach in the future

33%



of organizations don't test their mobile apps

...and traditional security practices are unsustainable

85



security tools from

45



vendors

1.5M

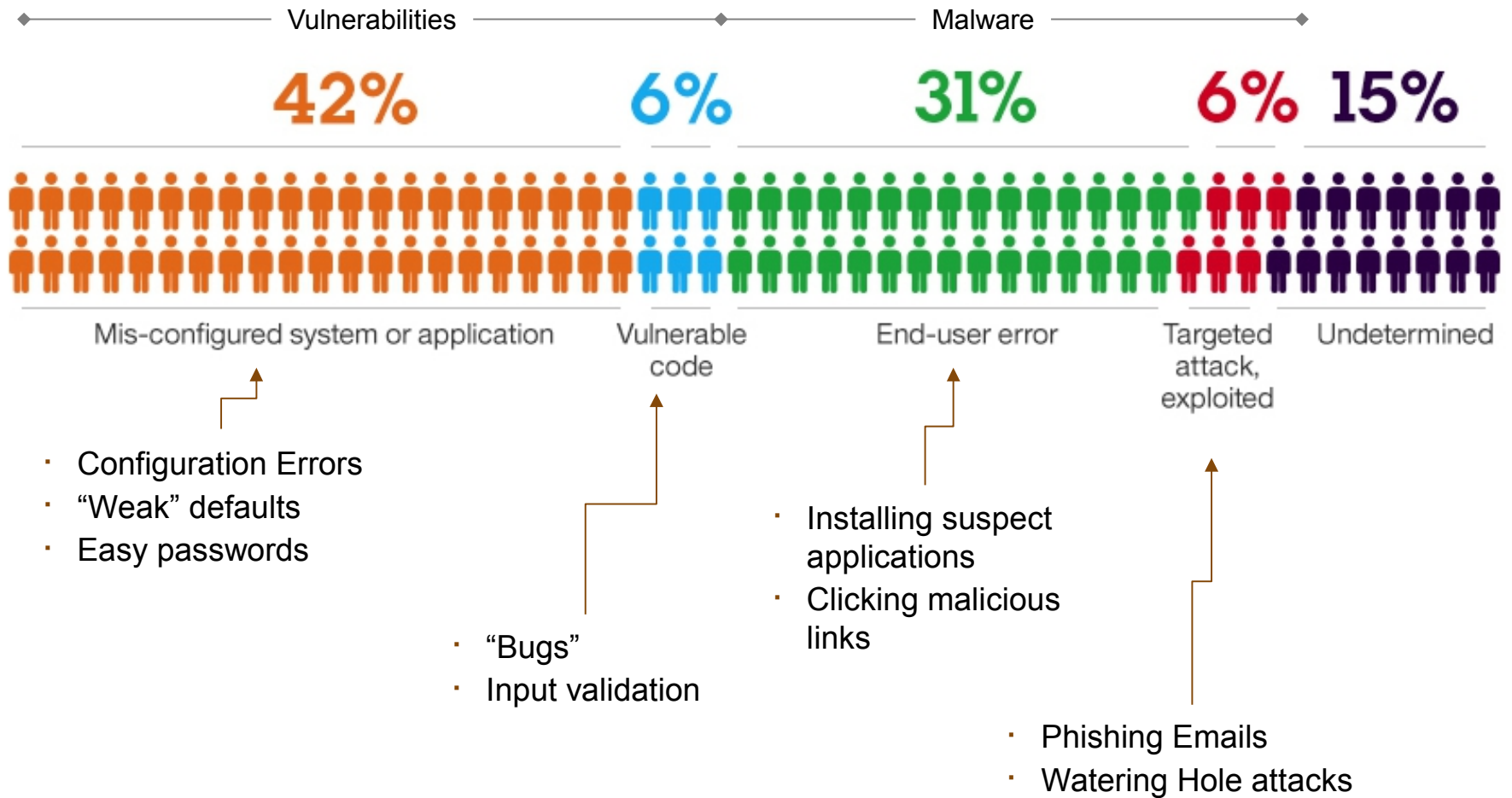


open and unfilled security positions by 2020

Key Trends from 2015



Why do Breaches Happen?



Source: IBM Security Services 2013 Cyber Security Intelligence Index

Security leaders are more accountable than ever before

CEO / COO

- Loss of market share and reputation
- Legal exposure
- Business continuity

CCO / CFO

- Audit failure
- Fines and enforcement impact
- Financial loss

CIO

- Impact to data and systems, *confidentiality, integrity / availability*

CHRO / CDO

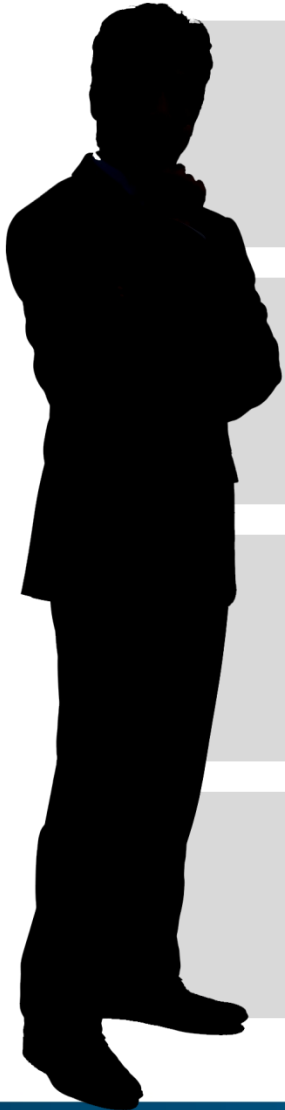
- Violation of employee privacy
- Loss of sensitive data

CMO

- Loss of brand reputation and customer trust

Your board
and CEO
demand a strategy

Key takeaways for **CISOs**



Don't forget the basics

scanning, patching, configurations, passwords

Social Defense needs Socialization

educate users and engender suspicion

Defragment your Mobile posture

constantly apply updates and review BYOD policies

Optimize ahead of Attackers

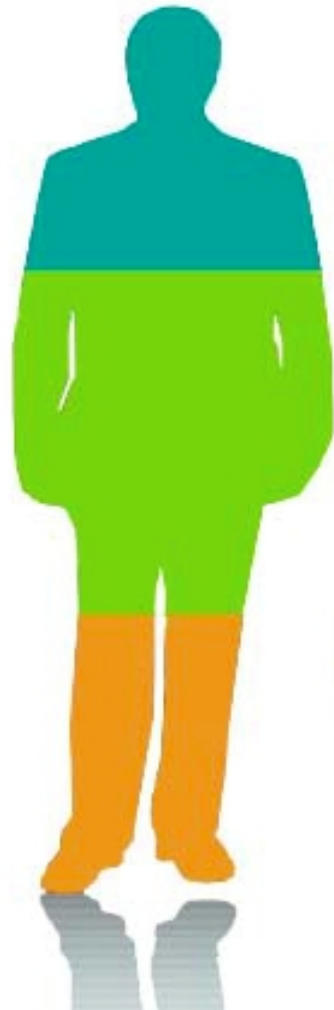
identify critical assets, analyze behavior, spot anomalies

- Make Security Strategy Your Own—
- Know your Risks



Frameworks rely on the CISO having Stakeholder Participation

And their roles are evolving with growing **authority**, **accountability** and **impact** across the enterprise.



Influencers

Confident and prepared, influence the business strategically

Protectors

Less confident, prioritize security strategically but lack necessary structural elements

Responders

Least confident, focus largely on protection and compliance

How they differ

have a dedicated CISO



have a security/risk committee



have information security as a board topic



use a standard set of security metrics to track their progress



focused on improving enterprise communication/collaboration



focused on providing education and awareness



IBM Center for Applied Insights, www.ibm.com/smarter/cai/security

Importance of metrics



Figure 4: Influencers are more likely to measure progress through a wider variety of metrics and devote more attention to systemic change than the other groups.

Security profiles



















		Responders	Protectors	Influencers
Structure and management	Dedicated CISO	 26%	 42%	 56%
	Security/risk committee	 26%	 52%	 68%
	Budget line item	 27%	 45%	 71%
	Budget authority	CIO (30%) IT VP/Director/Manager (24%) CFO (18%)	CIO (32%) CFO (20%) CEO (20%)	CIO (26%) CEO (26%) CISO (13%)
Organizational reach	Increased leadership attention	 50%	 68%	 77%
	Regular board topic	 22%	 58%	 60%
	Primary focus over next two years	New security technology (46%) Updating business processes (36%)	Employee education (53%) New security technology (42%)	Employee education (50%) Communications/collaboration (24%)
Measurement	Standardized metrics	 26%	 43%	 59%

Figure 2: Influencers are much more likely to have elevated information security to a strategic priority.

2014 U.S. State of Cybercrime Survey

The survey identified eight common deficiencies where spending and efforts lag:

1. **Most organizations do not take a strategic approach to cybersecurity spending**
2. Organizations do not assess security capabilities of third-party providers
3. Supply chain risks are not understood or adequately assessed
4. Security for mobile devices is inadequate and has elevated risks
5. Cyber risks are not sufficiently assessed
6. Organizations do not collaborate to share intelligence on threats and responses
7. Insider threats are not sufficiently addressed
8. Employee training and awareness is very effective at deterring and responding to incidents, yet it is lacking at most organizations

<http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.jhtml>

Co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March-April 2014

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

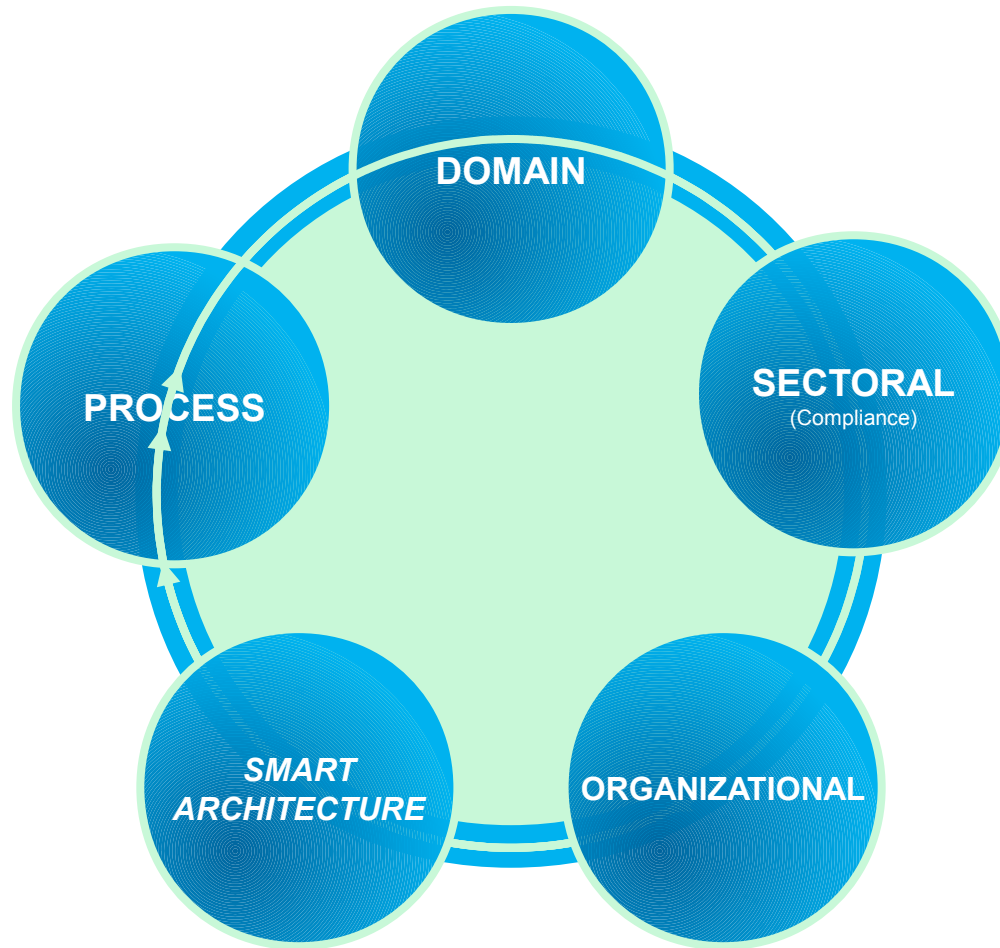
“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

*President Barack Obama
Executive Order 13636, Feb. 12, 2013*



- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

The Five Types of Security Risk Frameworks



NIST Cybersecurity Framework covers five core functions

Identify

- Develop an organizational understanding to manage cyber-security risk to systems, assets, data and capabilities
- Create an understanding of the business context, resources and risks so the organization can focus and prioritize its efforts

Protect

- Develop and implement safeguards to ensure delivery of infrastructure services and to help limit or contain the impact of a cyber-security event

Detect

- Develop and implement activities to identify the occurrence of a cyber-security event

Respond

- Develop and implement activities to take action following detection of a cyber-security event
- Support the ability to contain the impact of an event

Recover

- Develop and implement activities to maintain resilience and to restore capabilities or services impaired due to a cyber-security event
- Support timely recovery to normal operations

Reaching security maturity

Security Intelligence

Predictive Analytics, Big Data Workbench, Flow Analytics

SIEM and Vulnerability Management

Log Management

Advanced Fraud Protection

Optimized

Proficient

Basic

People	Data	Applications	Infrastructure
Identity governance Fine-grained entitlements Privileged user management	Data governance Encryption key management	Fraud detection Hybrid scanning and correlation	Multi-faceted network protection Anomaly detection Hardened
User provisioning Access management Strong authentication	Data masking / redaction Database activity monitoring Data loss prevention	Web application protection Source code scanning	Virtualization security Asset management Endpoint / network security management
Directory	Encryption	Application	Perimeter security

Incident response is time critical and cuts across the organization

Today's response is manual and disconnected

UNDEFINED RESPONSE PROCEDURES

create delays and unnecessary confusion

SILOED SECURITY TEAMS AND TOOLS

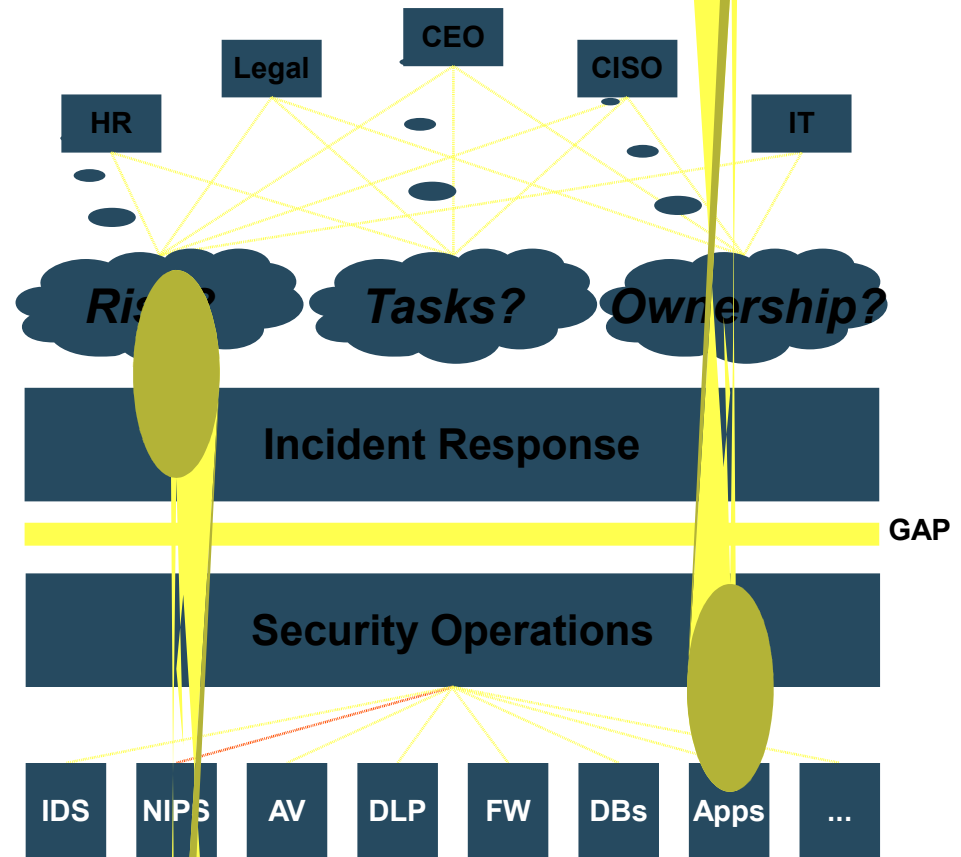
lead to manual activities and lost time

UNFAMILIARITY WITH REGULATIONS

cause unfulfilled obligations and privacy concerns

LACK OF SKILLS

build bottlenecks and an inability to act



IBM Leadership

- IT-SCC (Information Technology – Sector Coordinating Council), Member Executive Committee, Officer
- FIRST (Forum for Incident Response and Security Teams), Member Board of Directors
- IT-ISAC (Information Technology – Information Sharing & Analysis Center)
- ICASI (Industry Consortium for Advancing Security on the Internet), Member Board of Directors
- FS-ISAC (Financial Services – Information Sharing & Analysis Center)
- Other ISACs, Engines and Partners



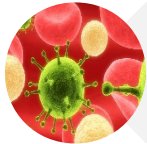
What can you do to mitigate these threats?



Keep up with threat intelligence



Maintain a current and accurate asset inventory



Have a patching solution that covers your entire infrastructure



Implement mitigating controls



Instrument your environment with effective detection



Create and practice a broad incident response plan



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security



IBM Security

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.