vital interacts

thinking inside & outside the box

CYBERSECURITY IN A WORLD OF CONNECTED DEVICES

Garry Barnes,
International Vice President, ISACA &
Practice Lead Governance Advisory
December 2015

vital interacts

What industry do you work in?

- **Government**
- **Banking/Financial services**
- **Power/utilities**
- **Telecommunications**
- **Health**
- **Education**
- **Technology sector**

How advanced is your knowledge of info/IT/cybersecurity?

- **basic**
- **intermediate**
- **advanced**

What are the cybersecurity challenges your industry faces?

Information security (traditional)

vital interacts

Preservation of:

- Confidentiality,
- Integrity, and
- Availability

Confidentiality

information is made available or disclosed to only those authorised.

Integrity

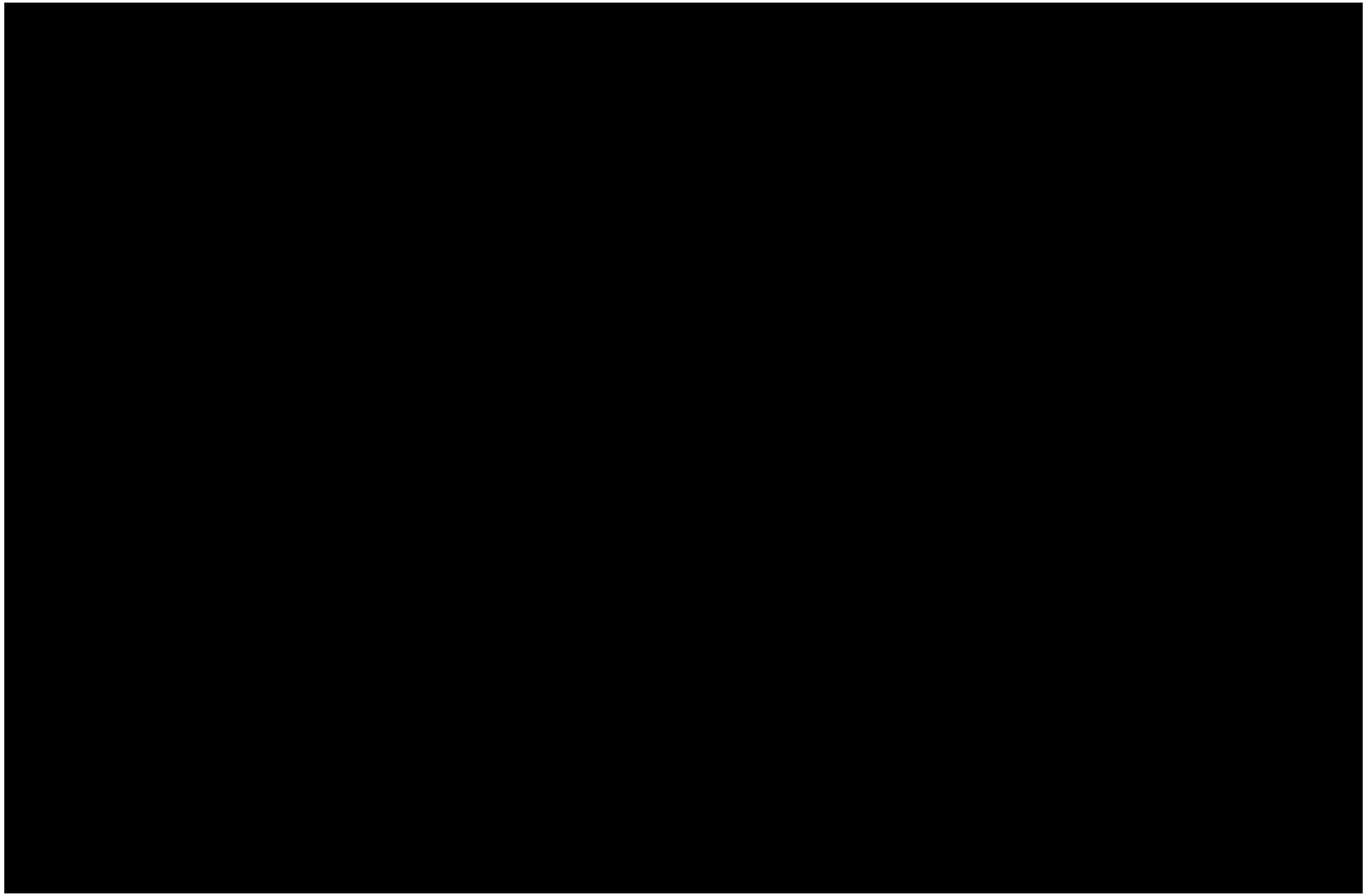
protecting the accuracy and completeness of information.

Availability

information is accessible and usable upon demand by an authorised entity.

Cybersecurity today

vital interacts

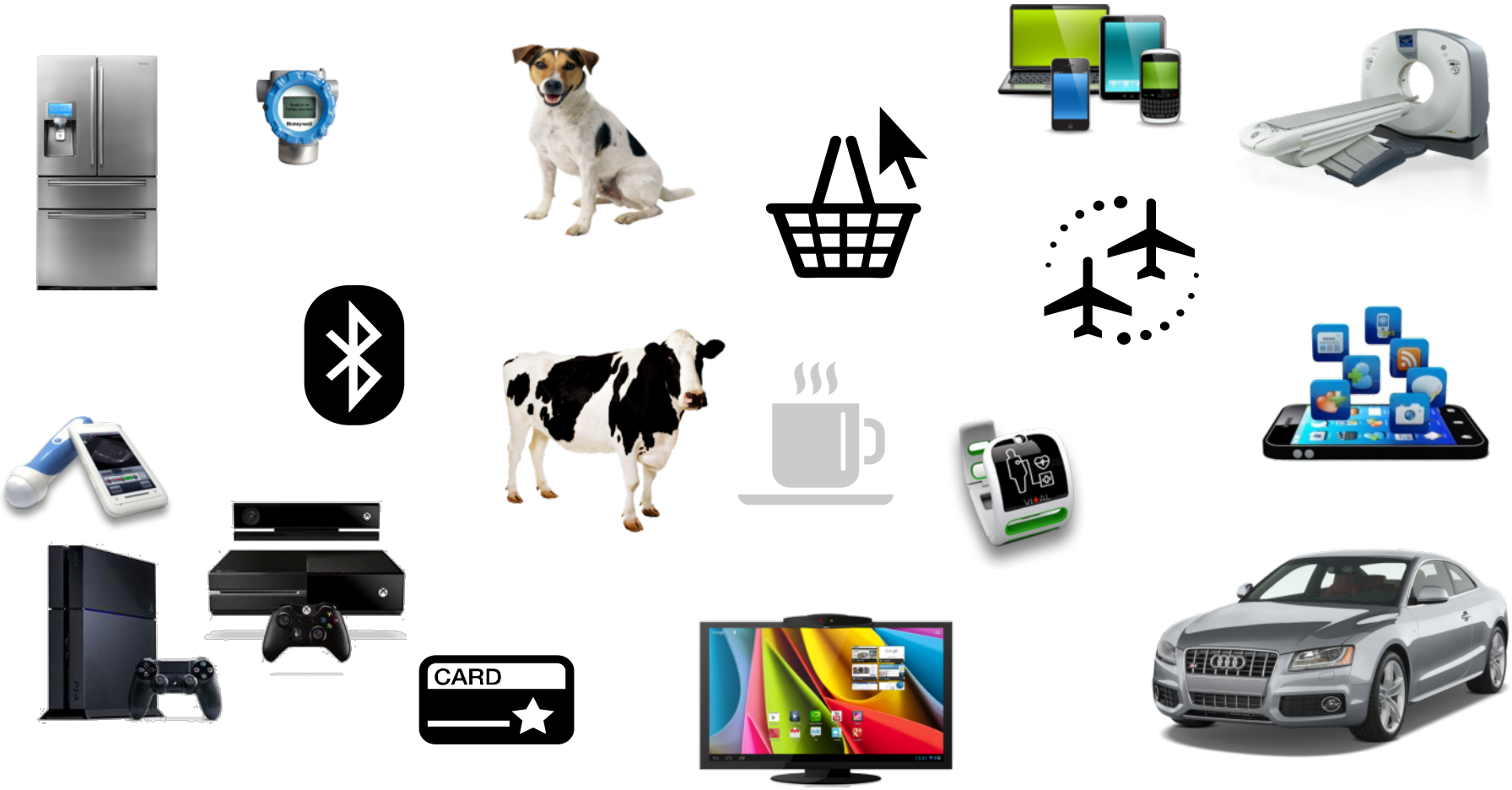


www.safeinternetbanking.be

Today's landscape

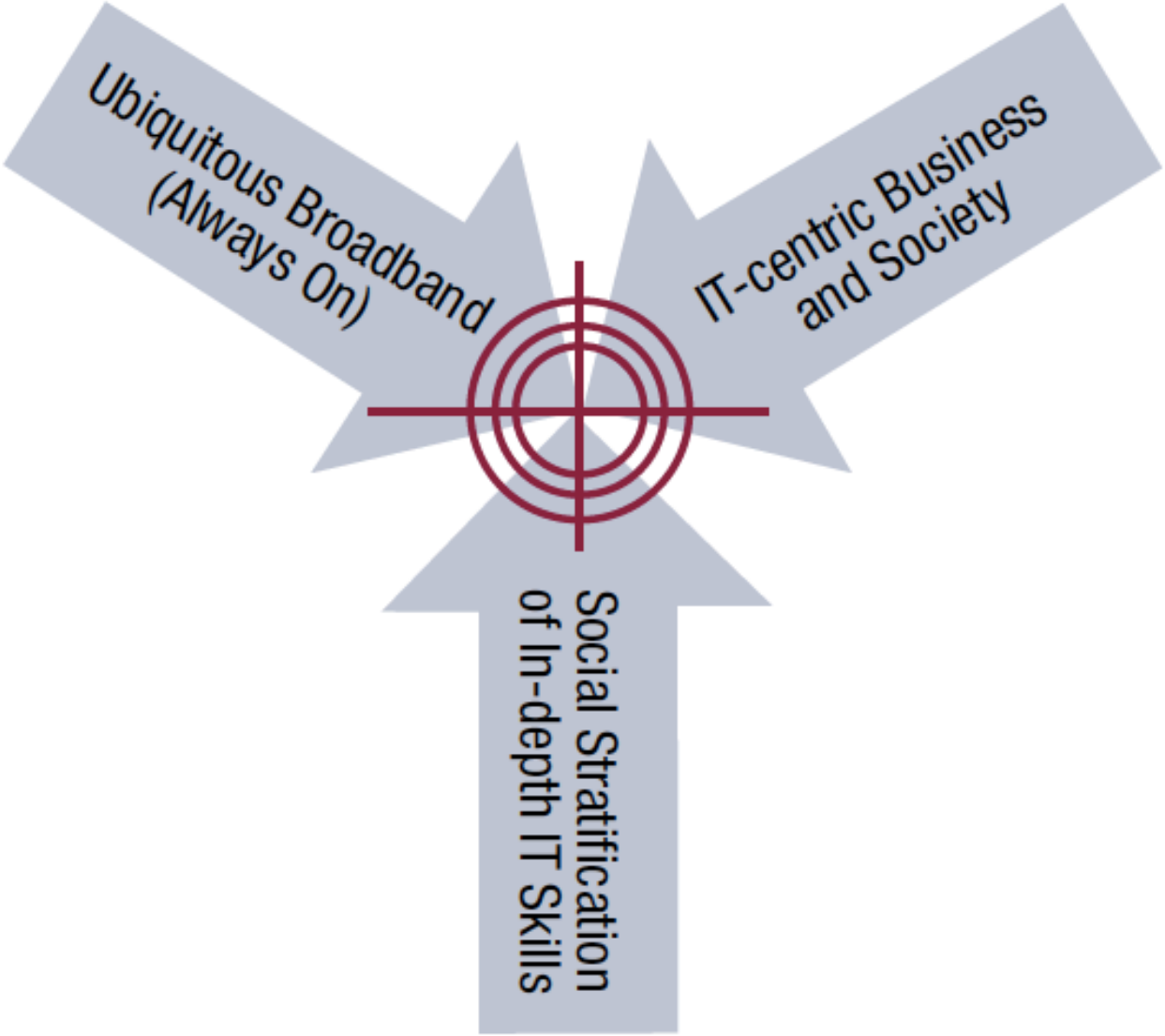
vital interacts

Technology is at the heart of most business, consumer and social interactions



Convergent game changers

vital interacts



Cybersecurity is frontpage news

vital interacts

itnews FOR AUSTRALIAN BUSINESS

News | Technology | Business | Awards | Labs | SC

Galleries | Research | Blogs | CXO Challenge | Topics | Resources | Events | Newsletter

Home / News / Technology / Security

Optus admits to three big d

Powered by SC Magazine

CSO — Mobile Security | Data Protection | Identity & Access | SecurityWatch | CSO Events | Resou

Sony hackers targeted employees with fake Apple ID emails

es of phishing
no were

CNN — International Edition | News | Regions | Video | TV | Features | Opinions | More… | London, United Kingdom 7° | Search CNN

U.S. | China | Asia | Middle East | Africa | Europe | Americas

World leaders' passport details rele
by immigration official

By Elizabeth Joseph, CNN

Updated 1433 GMT (2133 HKT) March 30, 2015

NEWS — LOCATION: Sydney, NSW Change

Just In | Australia | World | Business | Sport | Anal

Print | Email | Facebook | Twitter | More

Aussie Travel Cover has hundreds of thousands of records stolen in hacking, policy holders not informed

PM By Will Ockenden and Benjamin Sveen

The Sydney Morning Herald — Digital Life

Latest News | Gadgets | Science | Innovation | Web Culture | Gaming | Security | IT Pro

You are here: Home » Digital Life » Consumer Security »

Kids' data at risk as toymakers' tracking information is hacked

December 1, 2015 - 6:32AM | 9 reading now | Read later

Andrea Peterson

Tweet | submit | Email article | Print

R AUSTRALIAN BUSINESS

News | Technology | Business | Awards

alleries | Research | Blogs | CXO Challenge | Topics | Resources | Events | Newsletter

ome / News / Technology / Security

Hackers breach NSW GovDC web

Powered by SC Magazine

By Juha Saarinen on Mar 25, 2015 5:30 AM

Filed under Security

NEWS — LOCATION: Sydney, NSW Change

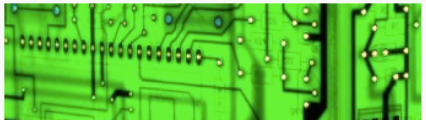
Just In | Australia | World | Business | Sport | Analysis & Opinion | Fact Check | Programs

China blamed for 'massive' cyber attack on Bureau of Meteorology supercomputer

By political editor Chris Uhlmann

Updated 56 minutes ago

China is being blamed for a major cyber attack on the computers at the Bureau of Meteorology, which has compromised sensitive systems across the Federal Government.



home › australia | world | opinion | sport | football | tech | culture | lifestyle | fa | all

Australian immigration and asylum

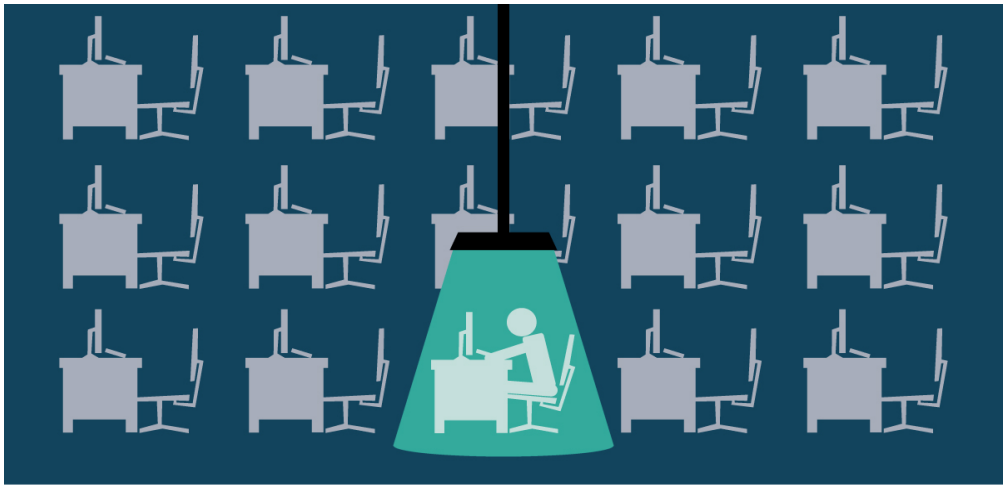
Asylum data breach: immigration unlawfully disclosed personal details

Privacy commissioner finds sensitive data on almost 10,000 asylum seekers was left publicly exposed for 16 days after the breach was reported

2015 Global cybersecurity status report

vital interacts

ISACA



83%
VIEW CYBERATTACKS AS ONE OF TOP 3 THREATS TO BUSINESS, BUT ONLY
38%
FEEL PREPARED FOR A SOPHISTICATED ATTACK
VISIT: WWW.ISACA.ORG/CYBERSECURITYREPORT

ISACA
Trust in, and value from, information systems
CSX™
CYBERSECURITY NEXUS

86%
SEE A CYBERSECURITY SKILLS SHORTAGE
VISIT: WWW.ISACA.ORG/CYBERSECURITYREPORT

ISACA
Trust in, and value from, information systems
CSX™
CYBERSECURITY NEXUS

www.isaca.org/cybersecurityreport

ISACA

vital interacts

ISACA's 2015 IT Risk/Reward Barometer

Global survey looks at cybersecurity in a world of connected devices

CSX™ CYBERSECURITY NEXUS

Two survey components:

- Consumer perspective—A separate five-country survey of nearly 5,400 consumers (Australia, India, Mexico, UK, US)
- IT/business perspective: A global survey of more than 7,000 business & IT professionals who are members of ISACA

Consumer perspective

vital interacts

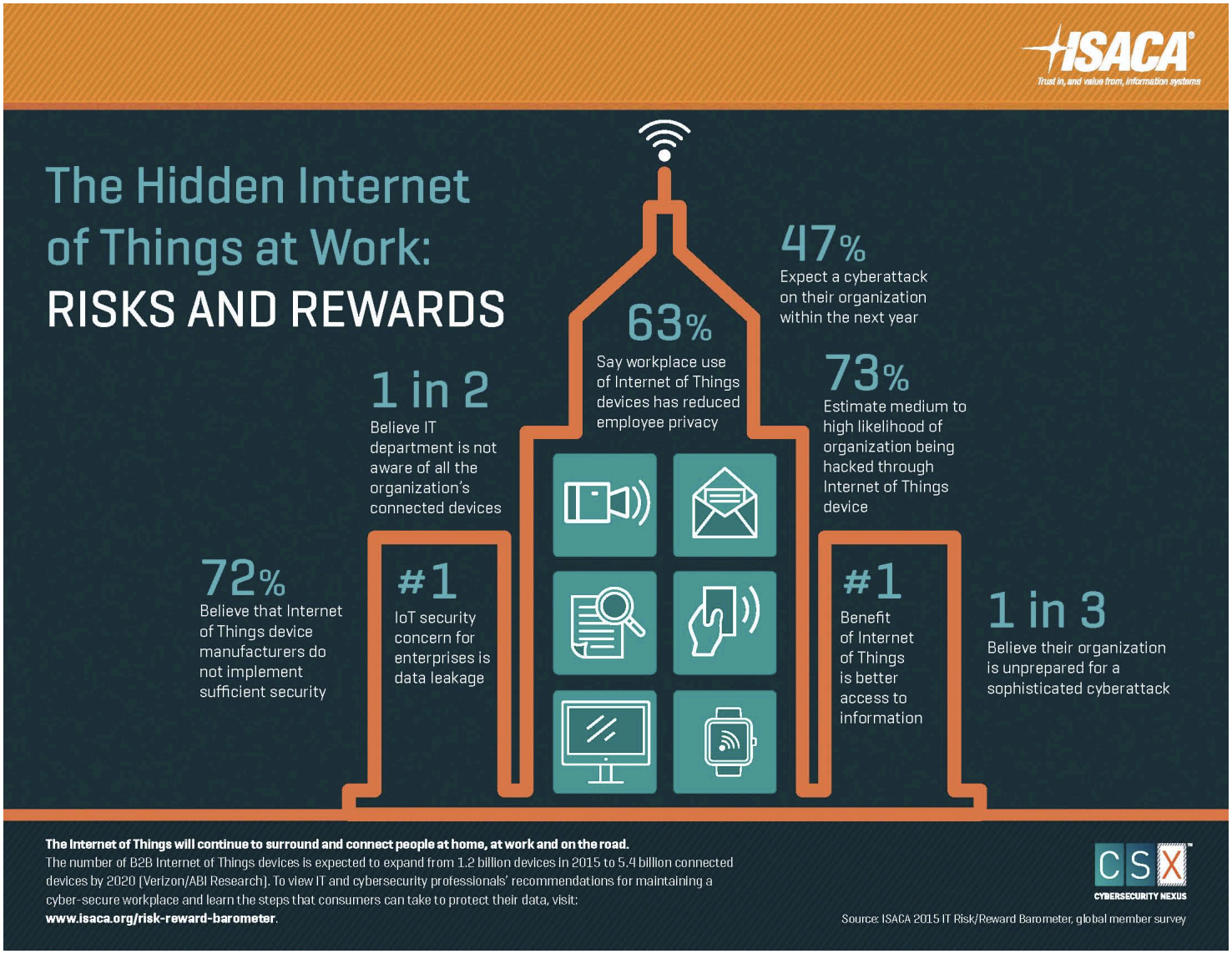
Consumers may feel over-confident about IoT security.

Business/IT perspective

vital interacts

Consumers may feel over-confident about IoT security.

IT & cyber security professionals are much less confident about it.



2015 ISACA APT Study

vital interacts

The Bad News:

- 28% have experienced an APT attack.
- Mobile device security lags, even though BYOD increases APT risk.
- Three-quarters of respondents report they have not updated their third-party agreements to ensure better protection against APTs.
- Organizations continue to prefer technical controls rather than education and training, even though many successful APT attacks gain entry through social engineering attacks.

The Good News:

- 62% indicate that their organizational leadership is becoming more involved in cybersecurity-related activities.
- 80% see a visible increase in support by senior management—a very positive first step in combating the APT.

www.isaca.org/apt-wp

ISACA

CYBERSECURITY CONCEPTS

What is cybersecurity?

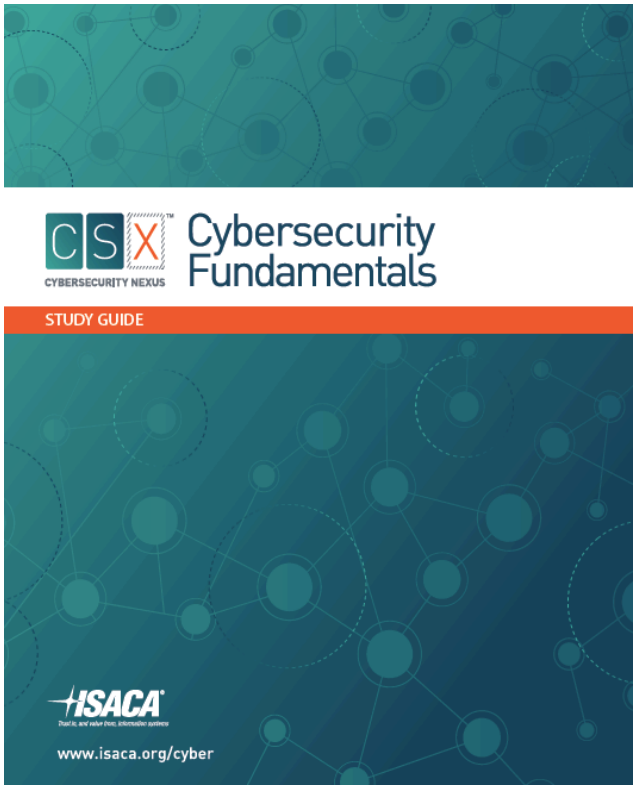
vital interacts

Various definitions exist

ISACA CSX Fundamentals:

Generally, cybersecurity refers to anything intended to protect enterprises and individuals from intentional attacks, breaches, incidents and consequences.

More specifically, **cybersecurity** can be defined as “the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.”



What is cybersecurity?

vital interacts

Various definitions exist

ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity:

“The preservation of confidentiality, integrity and availability of information in the Cyberspace”

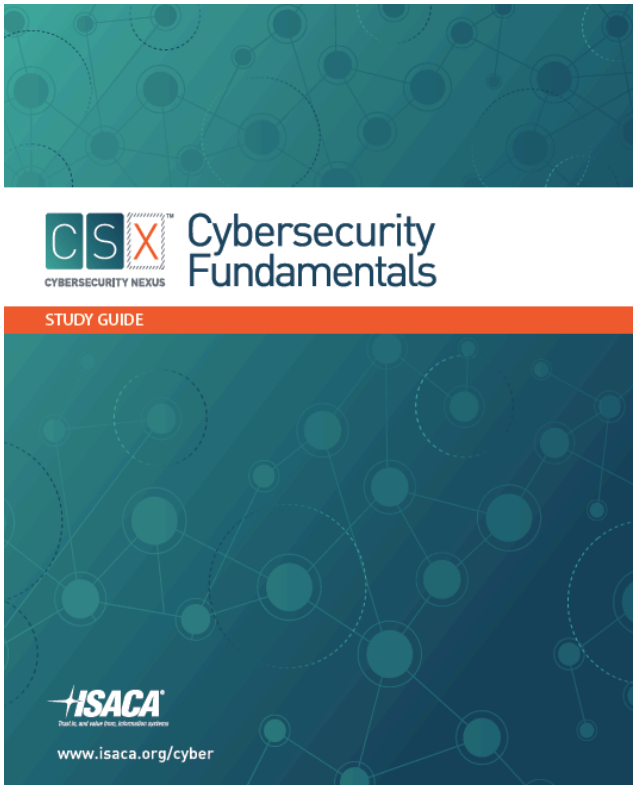
Cyberspace is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

ISACA's CSX Fundamentals

vital interacts

Core knowledge areas

1. Cybersecurity concepts
2. Security architecture principles
3. Security of networks, systems, applications and data
4. Incident response
5. The security implications of the adoption of emerging technologies

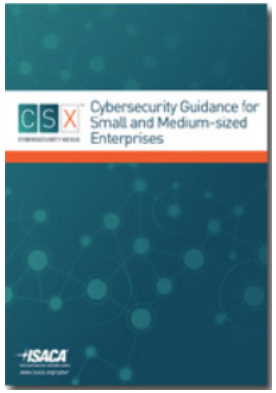


Cybersecurity guiding principles

vital interacts

Cybersecurity Guidance for Small and Medium-sized Enterprises

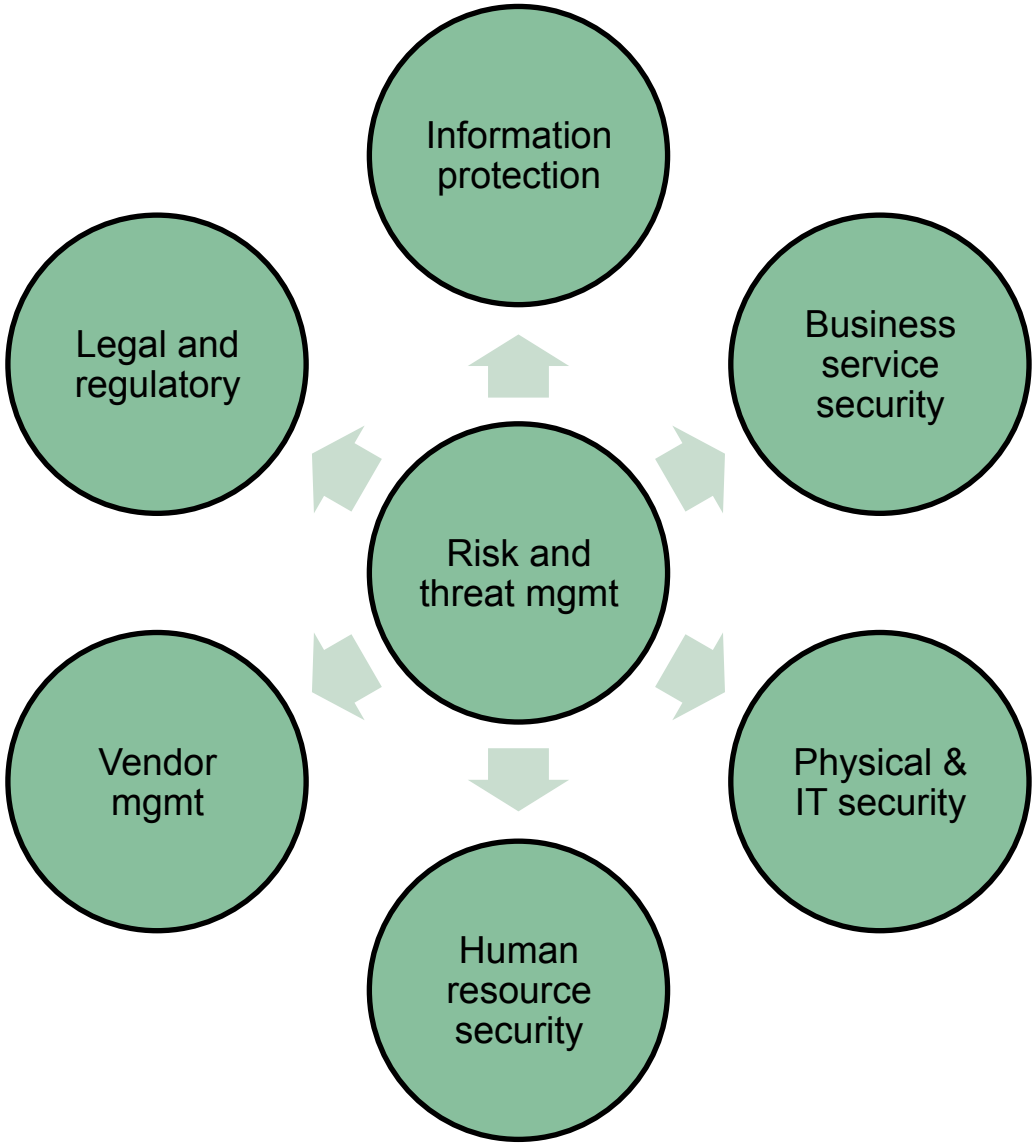
- **Principle 1: Know the potential impact of cyber attack**
- **Principle 2: Understand end users, their culture, values and behaviour patterns**
- **Principle 3: State the business case for cybersecurity and risk appetite for the enterprise**
- **Principle 4: Establish cybersecurity governance**
- **Principle 5: Manage cybersecurity using COBIT principles and enablers**
- **Principle 6: Know the cybersecurity assurance universe and objectives**
- **Principle 7: Provide reasonable assurance over cybersecurity**



Know the business impact

vital interacts

Potential focus areas for cyber risk and threat assessments



Understand the business context

vital interacts

What are the business drivers affecting cybersecurity?

External:

- Industry (financial, health, government, retail, utility, education, pharmaceuticals, agriculture etc.)
- Competitive environment
- Threat landscape
- Enterprise relationships, outsourcing and service providers
- Geo-political environment (including CERT capabilities, cyber policy, cyber crime, policing and forensic capabilities, etc.)
- Customers and clients

Internal:

- Information assets of value
- Internet-enabled services
- Security awareness, user behaviour and skills
- Security governance and management maturity
- Risk management maturity

Understand the technical context

vital interacts

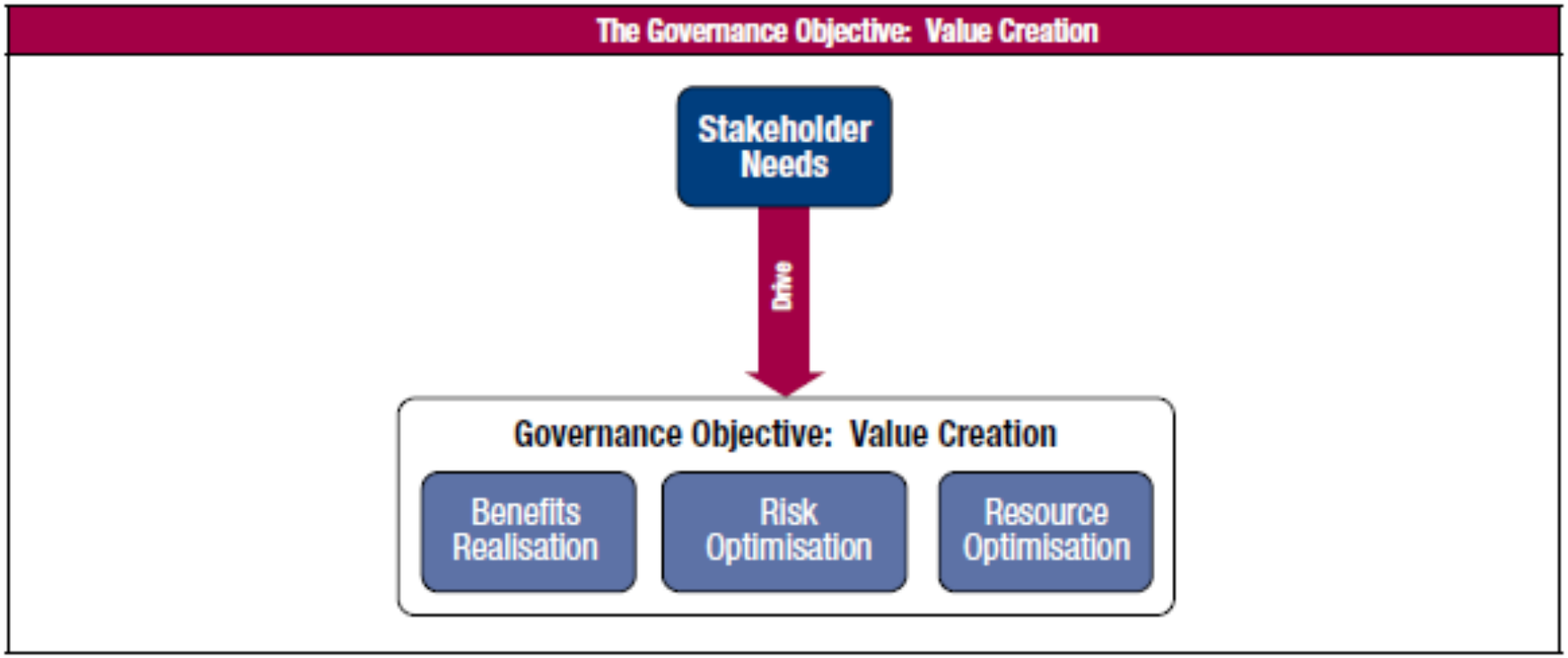
What are the technical drivers affecting cybersecurity?

- Network connectivity (with customers, partner organisations, service providers, data sharing services, etc.)
- Platforms and tools used (web platforms and applications, mobility, operating systems, databases, customer management systems, content management systems)
- Level of IT complexity and maturity
- Internal or managed IT and security services
- Use of cloud services
- Operational support for security
- Degree of technology change
- User community and capabilities
- New or emerging security tools

Establish security governance

vital interacts

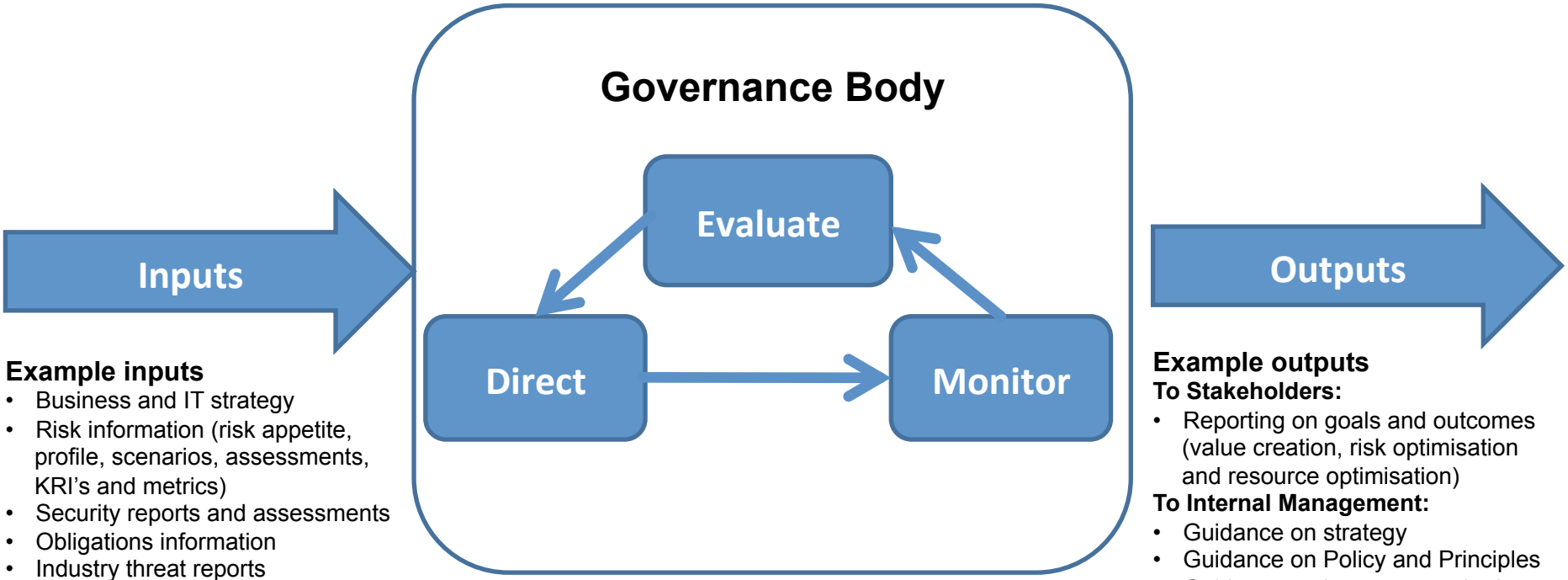
Governance objective: Value creation



COBIT® 5
AN ISACA® FRAMEWORK

Security governance

vital interacts



Example inputs

- Business and IT strategy
- Risk information (risk appetite, profile, scenarios, assessments, KRI's and metrics)
- Security reports and assessments
- Obligations information
- Industry threat reports
- Internal threat/risk reports
- Incident management reports
- Service provider risk assessments and reports

Example outputs

To Stakeholders:

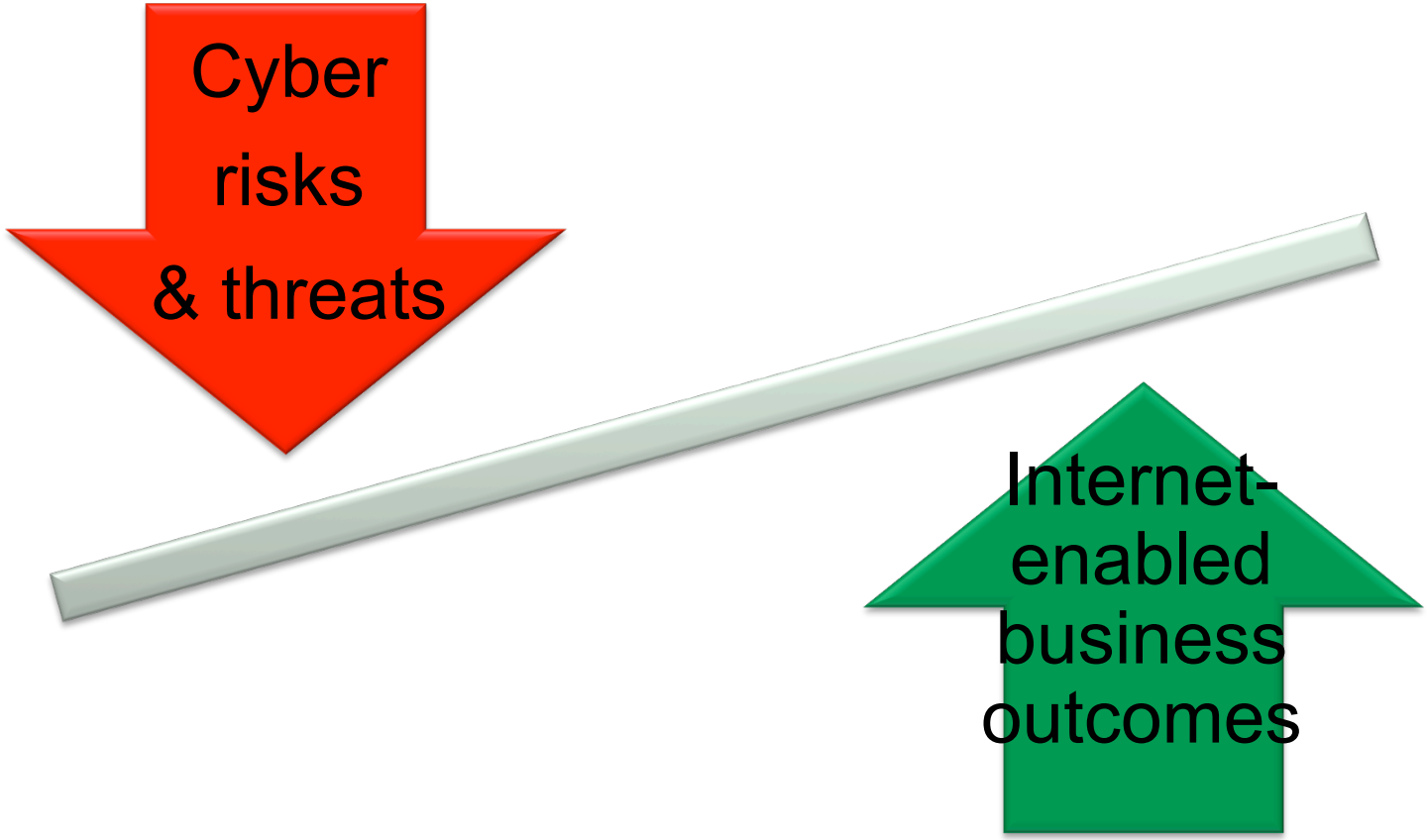
- Reporting on goals and outcomes (value creation, risk optimisation and resource optimisation)

To Internal Management:

- Guidance on strategy
- Guidance on Policy and Principles
- Guidance on investment criteria
- Guidance to risk owners
- Approved budget and structure
- Delegation of duties/tasks

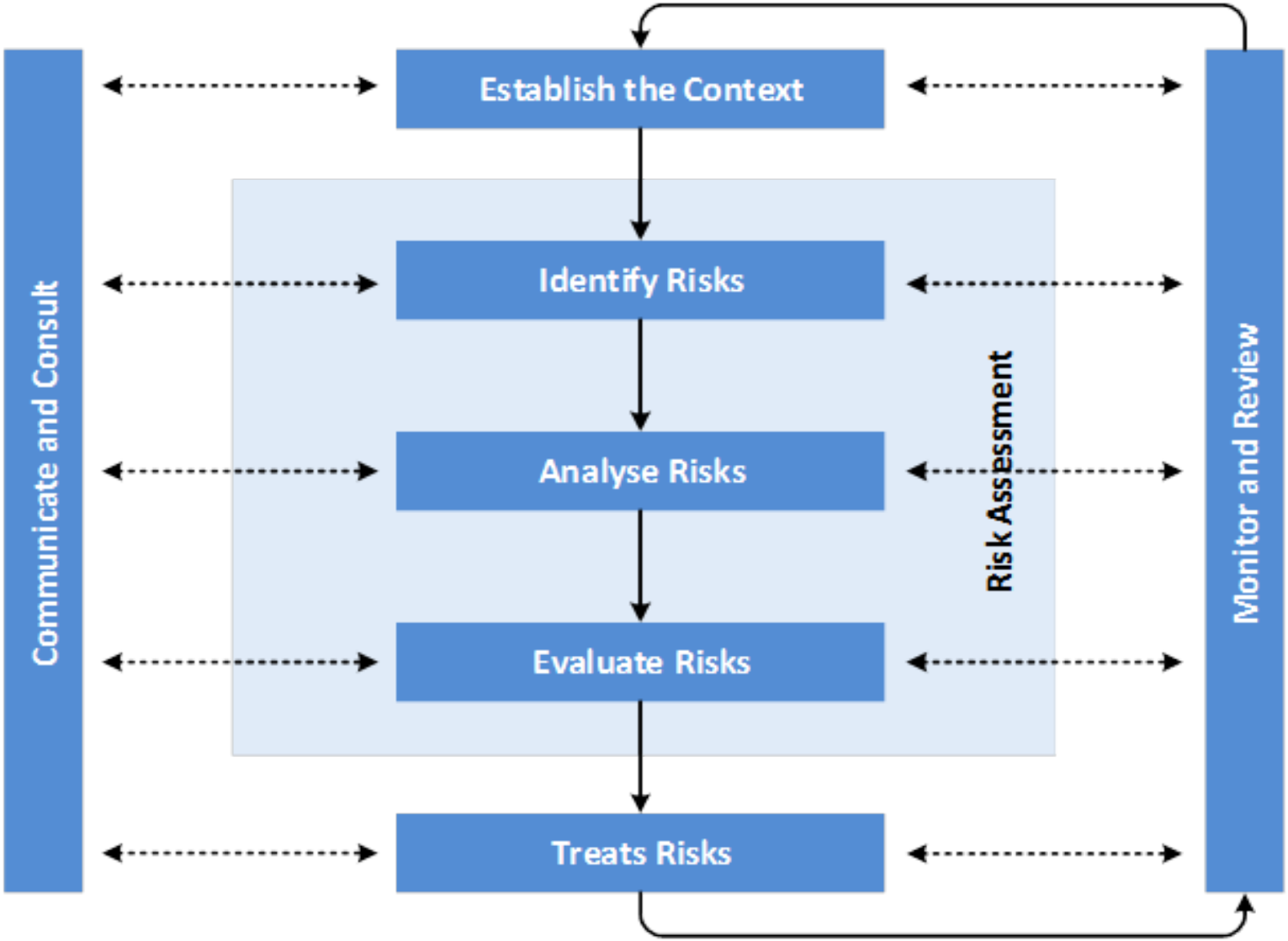
Align risk and opportunity

vital interacts



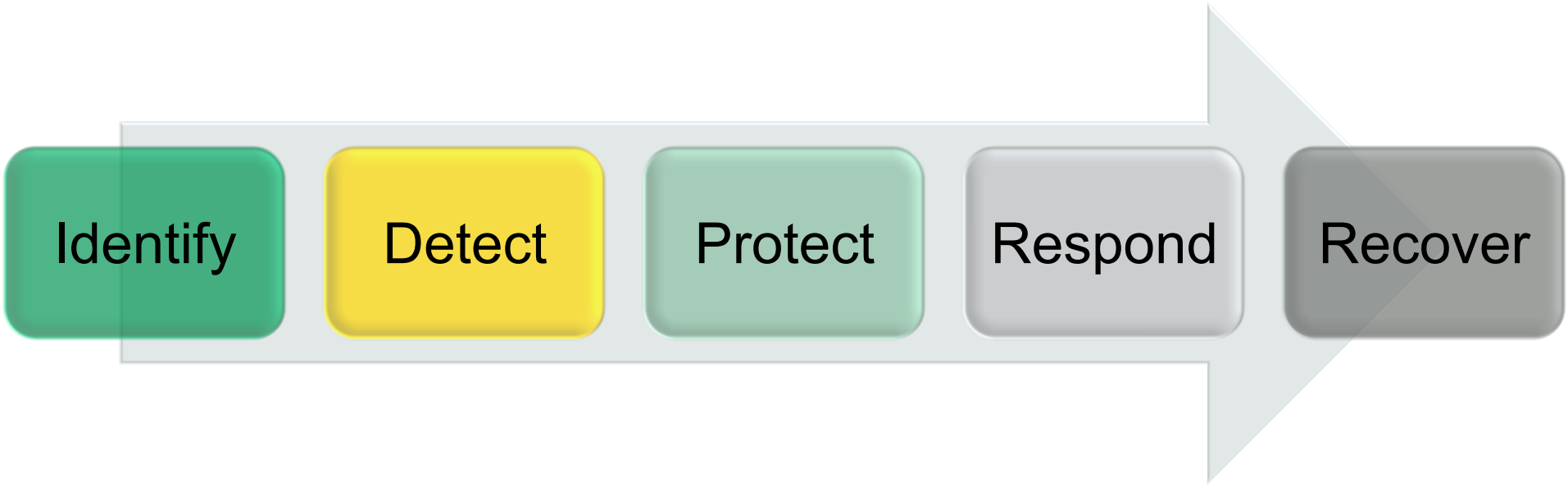
ISO31000 risk management process

vital interacts



Threat management

vital interacts



Understand the threat landscape

vital interacts

Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.

Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.

Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.

State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.

Risk

APT — State-sponsored Espionage and Weaponization

Insiders — Personal Gain

Hackers — Money

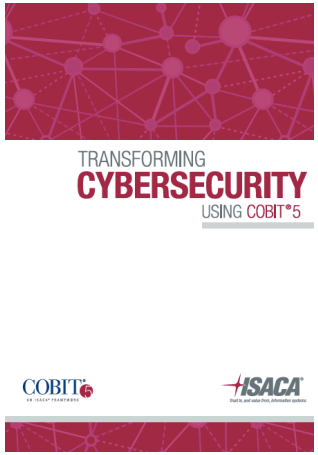
Script Kiddies — Amusement/ Experimentation/ Nuisance

APT Life Cycle: Intelligence Gathering → Initial Exploitation → Command and Control → Privilege Escalation → Data Exfiltration

Attacker Resources/Sophistication

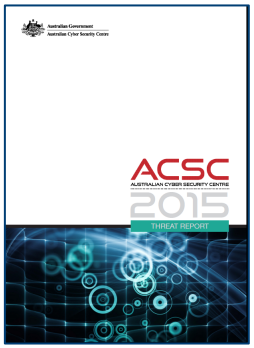
1980s/1990s → 2012

- BrainBoot/Morris Worm
- Polymorphic Viruses
- Michelangelo
- Concept Macro Virus
- Melissa
- "I Love You"
- Anna Kournikova
- Sircam
- Code Red and Nimda
- SQL Slammer
- Blaster
- Sobig
- MyDoom
- Netsky
- Sasser
- Storm botnet
- Koobface
- Conflicker
- Aurora
- Mariposa
- Stuxnet
- WikiLeaks
- Anonymous
- LulzSec
- SpyEye/Zeus
- Duqu
- Flame



Australian Cybersecurity Center 2015 Report

vital interacts



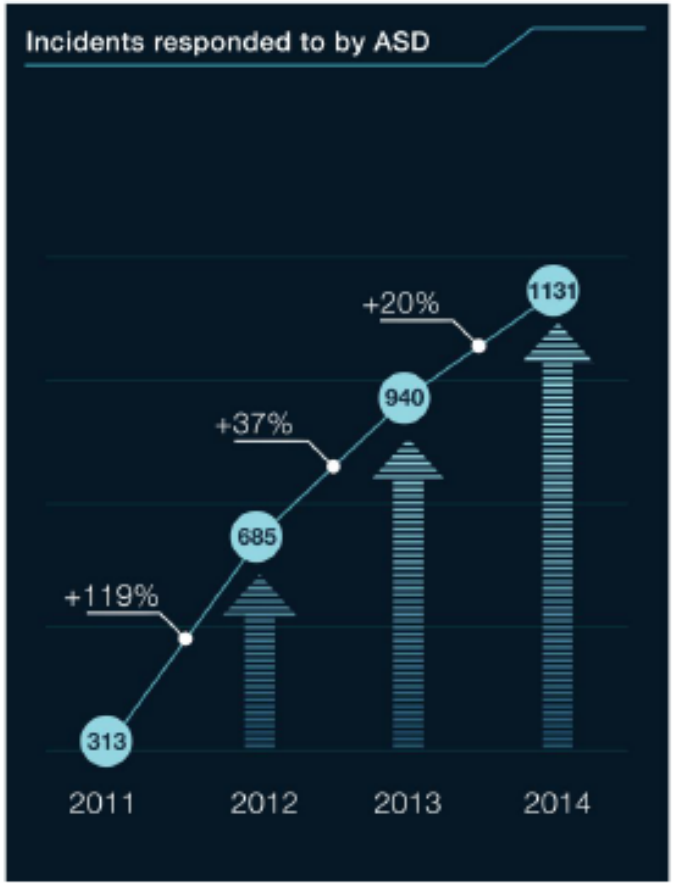


Figure 1: Cyber security incident responses by ASD

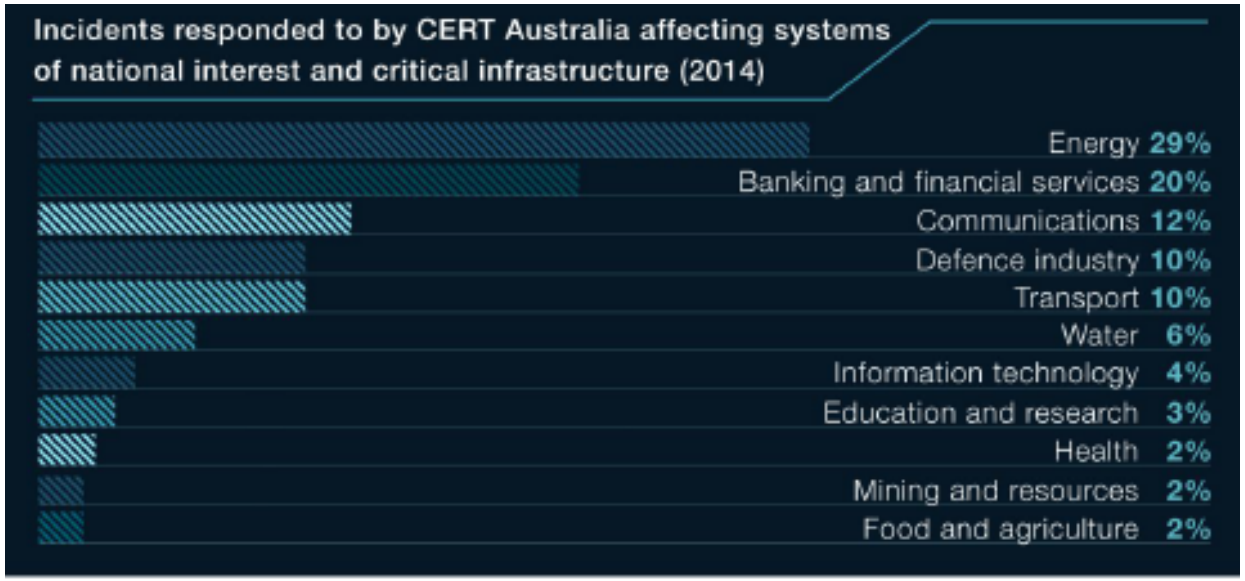


Figure 2: Incidents responded to by CERT Australia affecting systems of national interest and critical infrastructure in 2014

Cyber maturity in the Asia-Pacific Region 2015

vital interacts

https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015

FIJI

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	2
b) Is there legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	2
4 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	3
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	4
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of the population has internet connectivity?	5

Understand the detection lag

vital interacts

According to a recent Ponemon Institute study it took enterprises

170 days

on average to detect an attack by malicious outsiders and

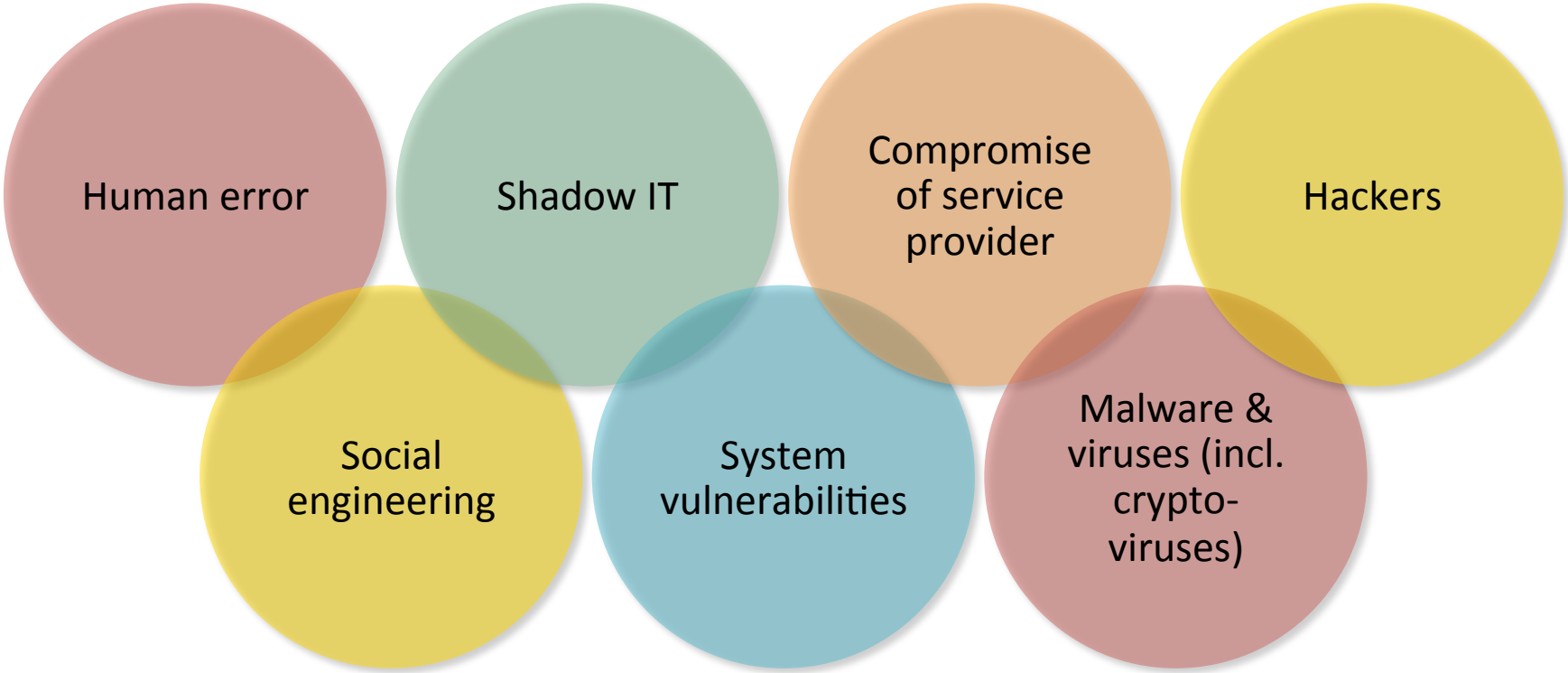
259 days

when insiders were involved in the attack.

Ponemon Institute, 2014 Global Report on the Cost of Cyber Crime

Threats & vulnerabilities

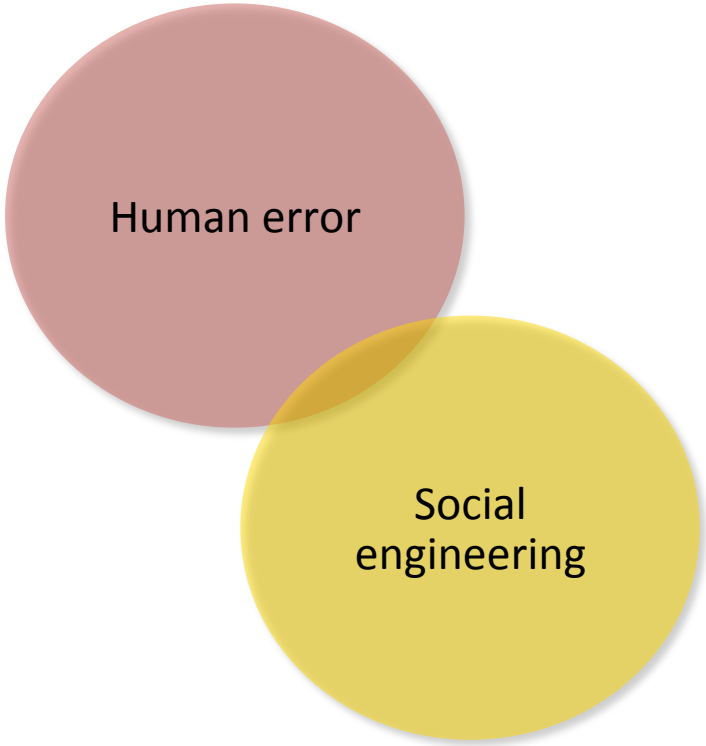
vital interacts



Quality risk and threat information is key to a successful cybersecurity program

Threats & vulnerabilities

vital interacts



Causes:

- lack of awareness and/or skills
- task saturation
- targeted attack to steal assets of value or compromise a service

Improvement strategies

- training and awareness
- policy and procedures
- explain the value of business information
- root cause analyses of incidents

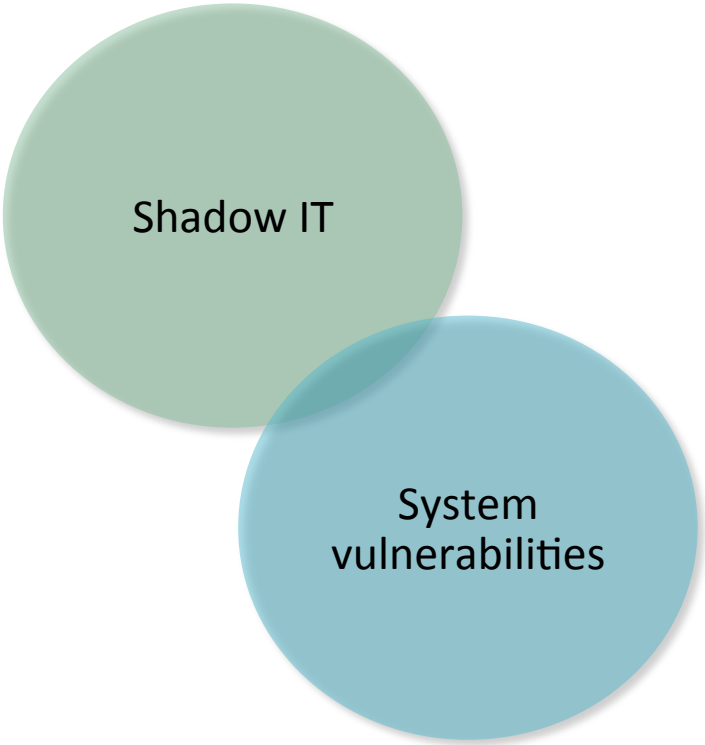
PEOPLE-BASED THREATS

Implications of our digital age

vital interacts

Threats & vulnerabilities

vital interacts



Causes:

- failure in procurement processes
- design errors
- poor patch and vulnerability management practices
- task saturation
- misaligned priorities

Improvement strategies

- training and awareness
- configuration policy and procedures
- secure by design
- root cause analyses of incidents

PROCESS WEAKNESSES

Computer “glitches” cause choas

vital interacts

The Daily Telegraph

National

Commonwealth bank outage causes chaos as customers left cashless

41 minutes ago

Gemma Wilson News Corp Australia Network

COMMONWEALTH Bank customers found themselves cashless when the company experienced major technical issues this morning.

ADVERTISEMENT

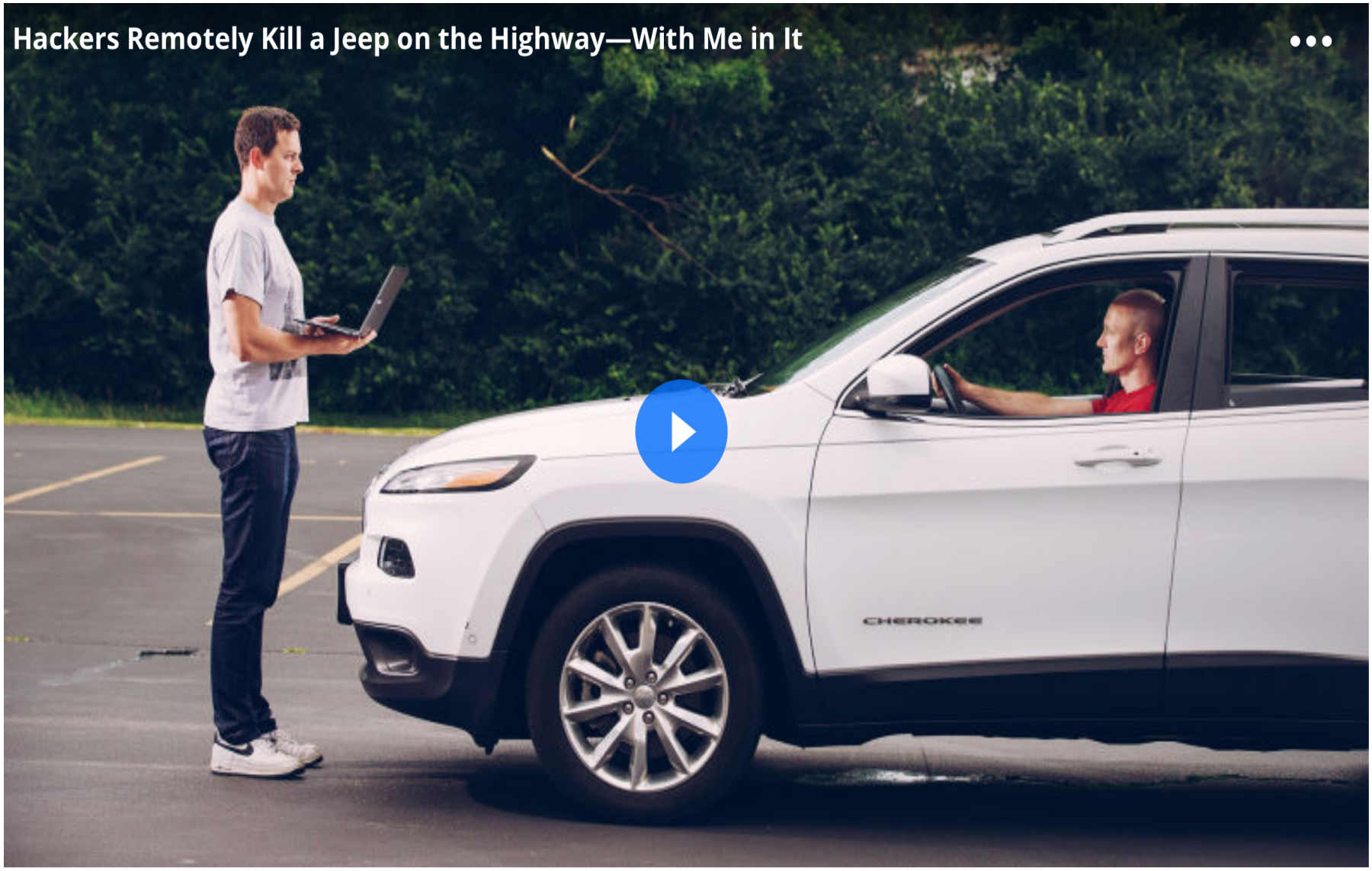
Most Viewed

LA Times

SEARCH

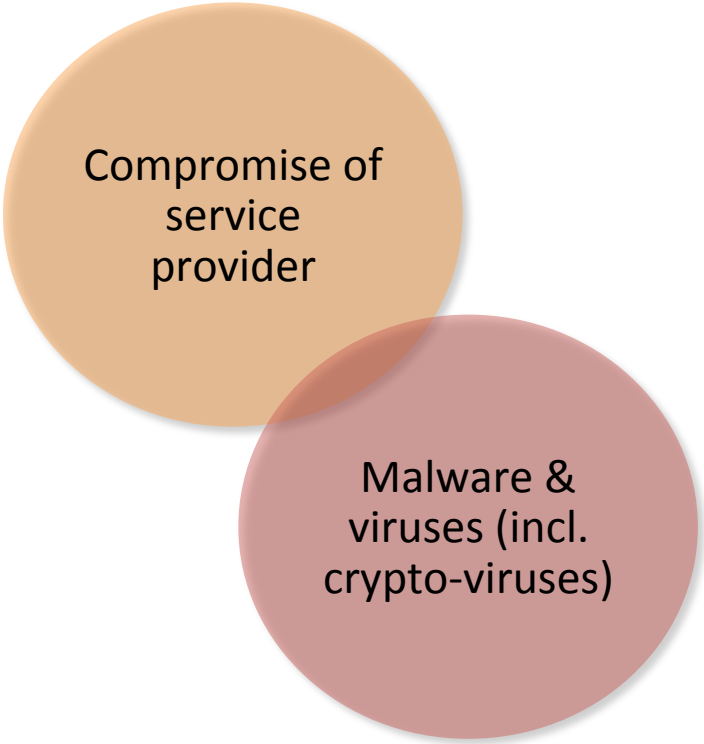
United Airlines blames grounding of hundreds of flights on computer glitch

vital interacts



Threats & vulnerabilities

vital interacts



Causes:

- control weaknesses
- misaligned priorities
- targeted attack to steal assets, obtain access or compromise a service

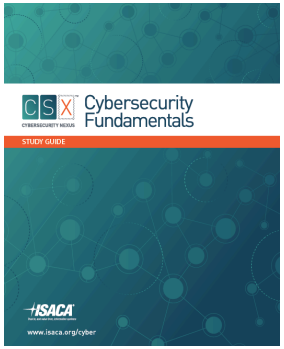
Improvement strategies

- training and awareness
- monitoring and audit of service providers
- data back-up and recovery testing

EXTERNAL THREATS

Malware

Malware, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.



Viruses
Worms
Trojan horses
Botnets
Spyware
Adware
Ransomware
Keyloggers
Rootkit

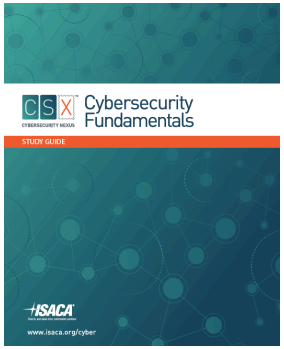
Ransomware and extortionware

vital interacts

Hackers sent extortion email to Sony executives 3 days before attack

Other attack types

Advanced persistent threats
Backdoor
Brute force
Buffer overflow
Cross-site scripting
Denial-of-service
Man-in-the-middle
Social engineering
Phishing
Spear phishing/whaling
Spoofing
SQL injection
Zero-day exploit



Threats & vulnerabilities

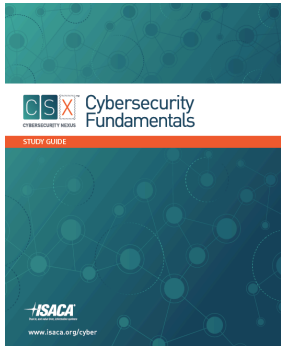
vital interacts

Threat agents:

- Corporations
- Nation states
- Hacktivists
- Cyberterrorists
- Cybercriminals
- Cyberwarriors
- Script kiddies
- Social hackers
- Employees (internal)

EXTERNAL THREATS

Attack attributes



vital interacts

Attack vector → Payload → Exploit → Vulnerability → Target (asset)

Path of attack: ingress (external attacker) or egress (data exfiltration)

Container carrying exploit code (email, malware)

Code used to execute attack

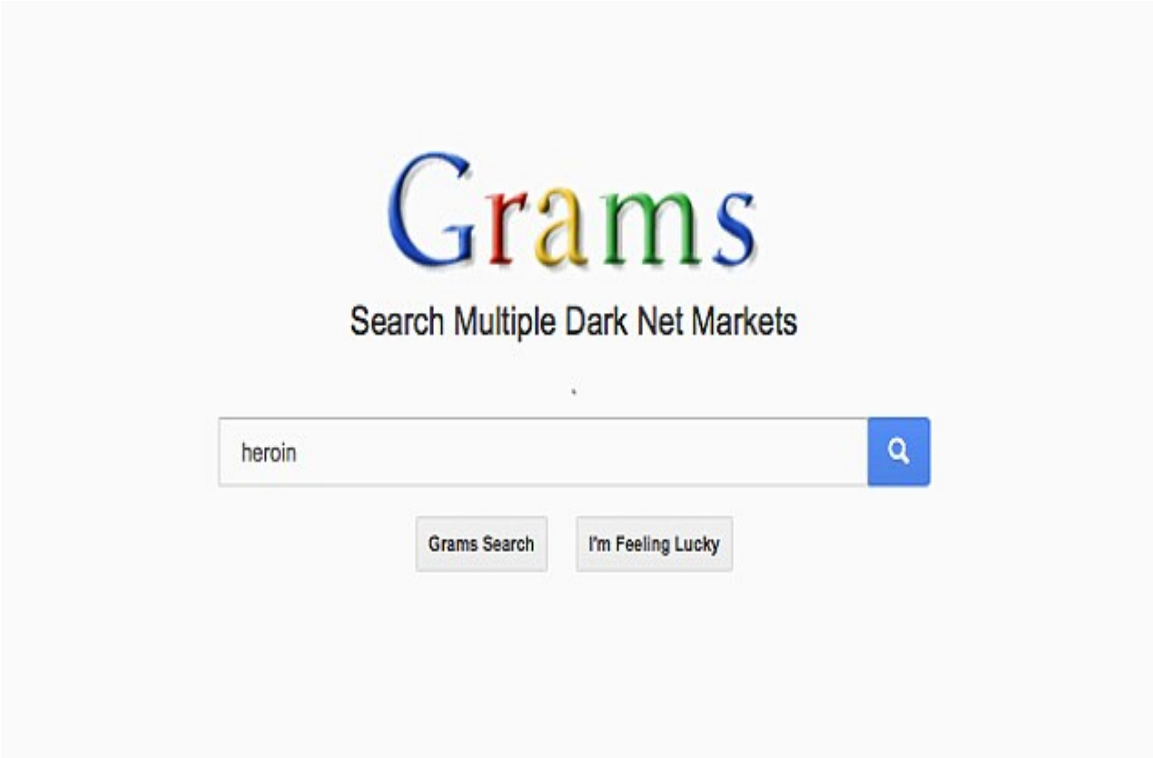
Weakness in process or code

Objective

Attack objective may be to enable a subsequent attack vector

Dark web

vital interacts



vital interacts

NORSE

ATTACK ORIGINS

	COUNTRY
100	United States
81	China
37	Netherlands
16	Russia
16	Brazil
13	India
5	South Korea
5	Hong Kong
4	Cyprus
4	Poland

Norse Dark Intelligence

Every second, Norse collects and analyzes live threat intelligence from darknets in hundreds of locations in over 40 countries. The attacks shown are based on a small subset of live flows against the Norse honeypot infrastructure, representing actual worldwide cyber attacks by bad actors. At a glance, one can see which countries are aggressors or targets at the moment, using which type of attacks (services-ports).

Hovering over the **ATTACK ORIGINS**, **ATTACK TARGETS**, or **ATTACK TYPES** will highlight just the attacks emanating from that country or over that service-port respectively. Hovering over any bubble on the map, will highlight only the attacks from that location and type. Press **$** to toggle table sizes.

Norse exposes its threat intelligence via high-performance, machine-readable APIs in a variety of forms. Norse also provides products and solutions that assist organizations in protecting and mitigating cyber attacks.

For more information, please contact: inquiry@norse-corp.com

Linked In **Facebook** **Twitter** **YouTube** **Google+**

- Each particle represents an attack
- Attack origins are grouped into clusters

25 200

- Countries are shaded in as they're attacked

25 100 500

By the Norse Corporation and Thomas dk Pocketknife. Many thanks to ArtZub for inspiration and the luminous particle. Built with d3 and the GoSquared Flag Icon Set.

vsn 1.1

LIVE ATTACKS

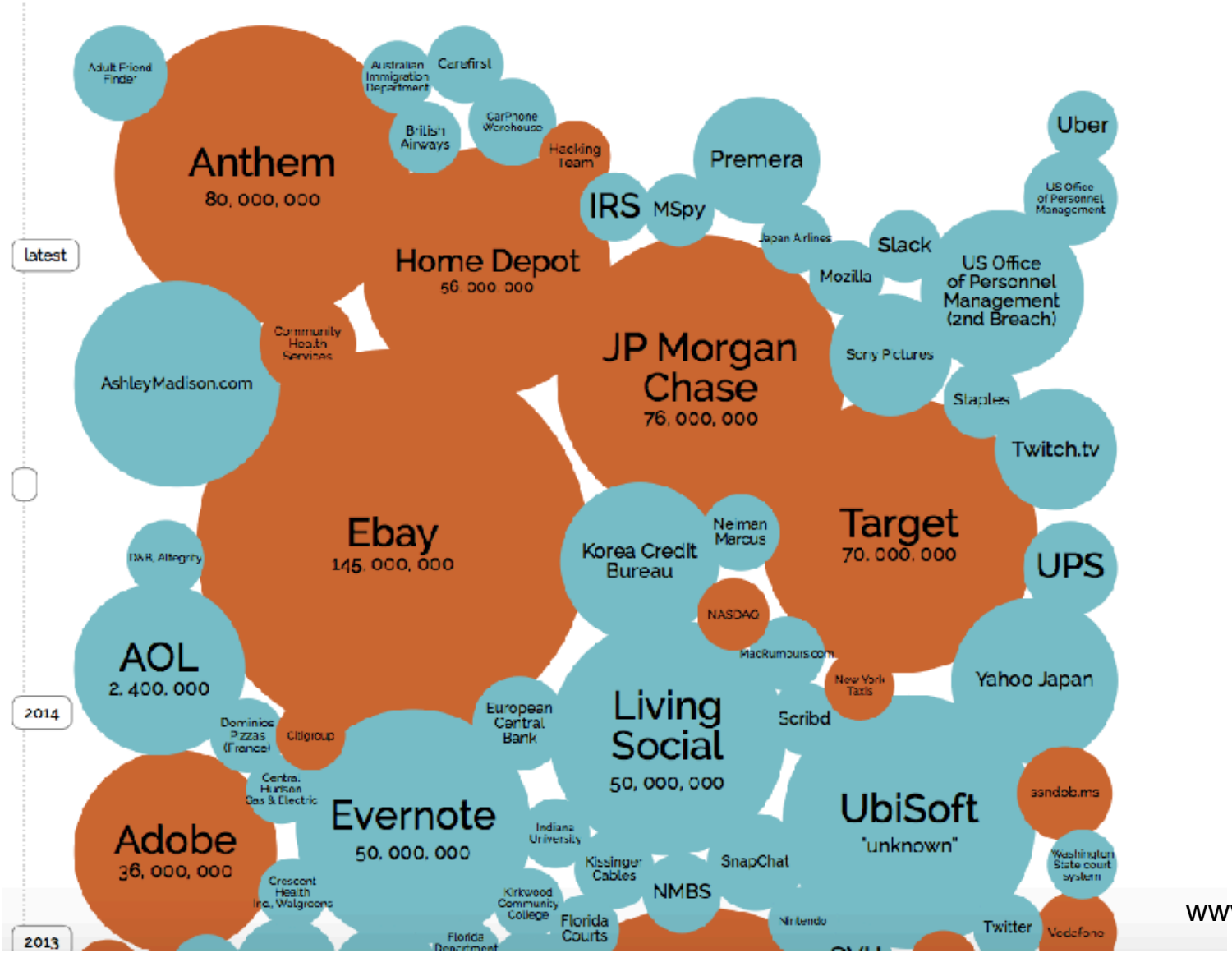
TIMESTAMP	ATTACKER ORGANIZATION	LOCATION	IP	TARGET LOCATION	TYPE SERVICE	PORT
2015-11-30 10:54:39.16	Golden Telecom	Dnipropetrovsk,	188.163.11.41	Lynnwood, United	microsoft-	445
2015-11-30 10:54:39.42	Ip Pool For Ppp Users	Baku, Azerbaijan	89.219.56.200	Lynnwood, United	ms-wbt-	3389
2015-11-30 10:54:39.43	Ip Pool For Ppp Users	Baku, Azerbaijan	89.219.56.200	Lynnwood, United	ms-wbt-	3389
2015-11-30 10:54:39.82	Asmanfaraz Sepahan Isdp	Esfahan, Iran	93.126.34.162	Kirksville, United States	ms-wbt-	3389
2015-11-30 10:54:40.42	China Unicom Shandong	Linyi, China	112.251.52.158	Lynnwood, United	unknown	50864
2015-11-30 10:54:40.42	Chinanet Guangdong	Shenzhen, China	121.35.86.99	Kirksville, United States	telnet	23
2015-11-30 10:54:40.67	Chinanet Guangdong	Shantou, China	183.7.130.62	Lynnwood, United	unknown	50856
2015-11-30 10:54:40.93	213.169.149.0-Pa	Nicosia, Cyprus	213.169.149.254	Nicosia, Cyprus	db-lsp-	17500

ATTACK TYPES

	SERVICE	PORT
38	telnet	23
27	microsoft-ds	445
24	unknown	50864
20	unknown	53413
18	rfb	5900
17	unknown	50856
13	ftp	21
13	netbios-ns	137

Who is affected?

vital interacts



www.informationisbeautiful.net/

vital interacts

SECURITY LAYERS

Information security program

vital interacts

GOVERNANCE ACTIVITIES

Ensures that Information Security is aligned with business goals and risk appetite

RISK MANAGEMENT

Effective information security risk enables assessing the target and current states and selecting appropriate response and reporting activities

INFORMATION SECURITY MANAGEMENT

Information Security Management practices that provide repeatable and holistic design, management and reporting of security and privacy controls

SECURITY OPERATIONS

Operational processes and controls enable security goals to be met while optimising risk.

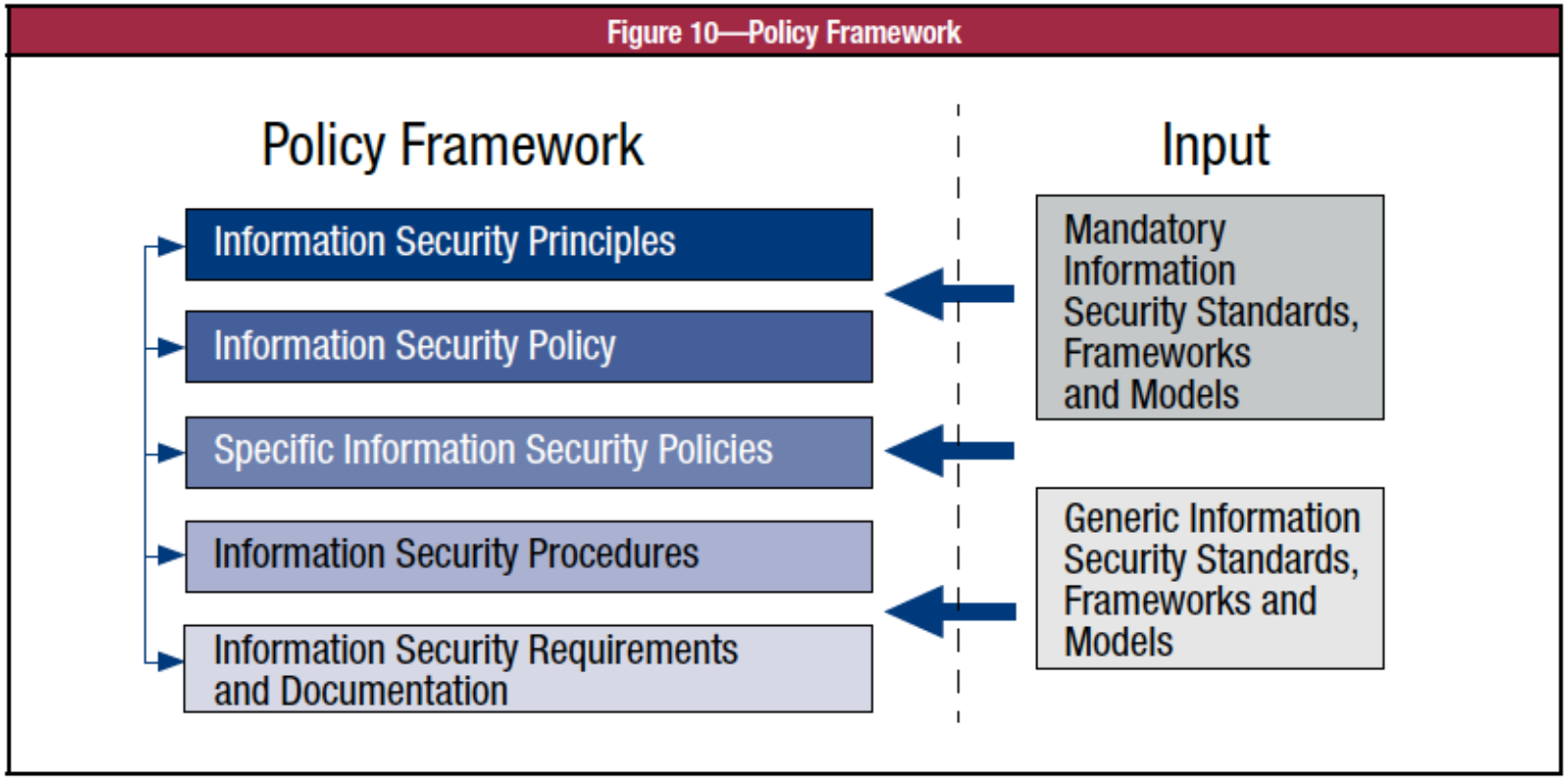
INCIDENT MANAGEMENT

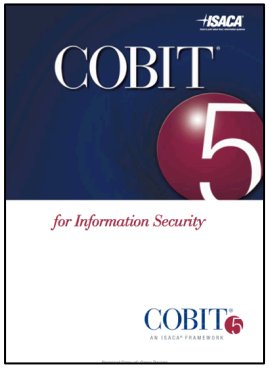
Incident response processes that identify, prevent, detect and correct security-related incidents.

Cybersecurity controls

vital interacts

Policy Framework

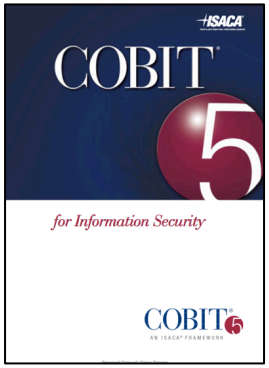




Cybersecurity controls

vital interacts

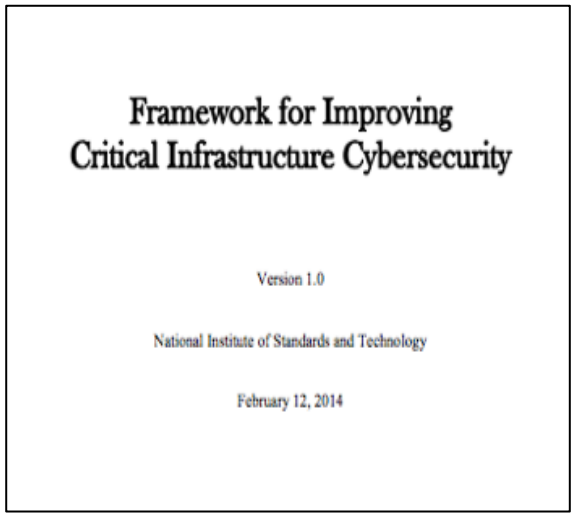
Key cybersecurity policies and processes



- Information Security Policy
  - People policies:
    - Personnel security
    - Acceptable use
    - Access, identity and authentication
  - Technical policies:
    - Security architecture
    - Configuration and patch management
    - Change management
  - Supplier/Third Party management
  - Systems development and acquisition
  - Testing and security assurance
  - Business Continuity, Disaster Recovery and Incident response

NIST Cybersecurity Framework

vital interacts

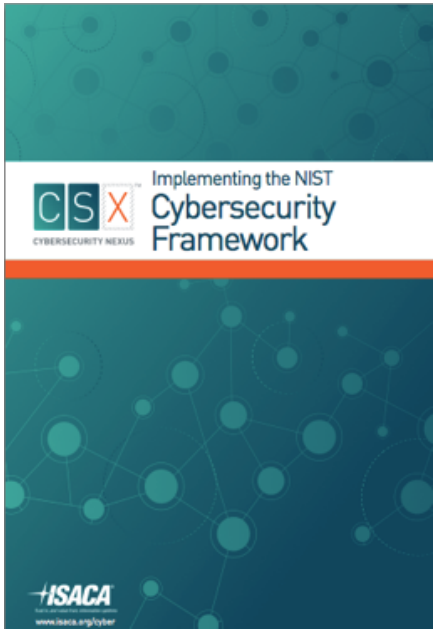

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

- **Implementing the NIST Cybersecurity Framework**
- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan



NIST Cybersecurity Framework

vital interacts

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

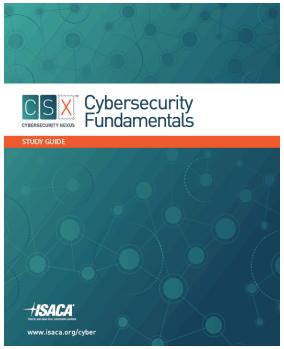
February 12, 2014

Table 1: Function and Category Unique Identifiers

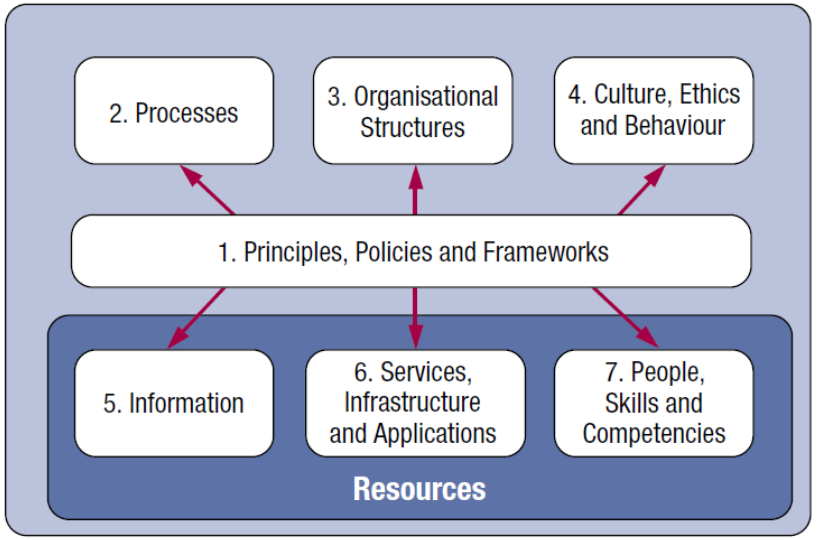
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Security architecture concepts

vital interacts



- **Defence in depth**
- **Defence in breadth**
- **Security perimeter**
- **Security architectures and frameworks**
  - SABSA
  - Zachman Framework
  - The Open Group Architecture Framework (TOGAF)



Cloud deployment models

vital interacts

Figure 4—Cloud Deployment Models	
Deployment Model	**Description**
Private cloud	• Operated solely for one enterprise • May be managed by the enterprise or a third party • May exist on- or off-premise
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services
Community cloud	• Shared by several enterprises • Supports a specific community that has a shared mission or interest • May be managed by the enterprises or a third party • May reside on- or off-premise
Hybrid cloud	A combination of two or more cloud deployment models (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability, e.g., cloud bursting for load balancing between clouds

Authentication & social engineering

vital interacts

OTP

Key security layers

vital interacts

1. **External perimeter**: ISP controls, cloud providers, Managed Security Services, external mail filtering and anti-spam solutions
2. **Corporate perimeter**: ingress/egress filtering, intrusion prevention/detection, threat management, vulnerability and penetration tests
3. **Logging and correlating network events**: using Security Information and Event Management System, Network Access Control and Network Intrusion Prevention/ Detection reporting.
4. **User behaviour:** authentication systems, awareness and training, user experience ("UX")
5. **Internal network controls**: configuration, segmentation, antivirus, application whitelisting, sandboxing
6. **Data protection**: access control, privileged account management, data encryption, logging
7. **Resilience, response and recoverability**: BCP/DRP, resilient architecture, application, system and data back-up, test of backups and restoration processes
8. **Threat intelligence**: Threat advisory services, threat analytics, OSINT

Incident Response stages

vital interacts

Incident Identification
Incident detection and reporting

→

Damage Assessment
Initial assessment and containment

→

Crisis Management
Management of the response

↓

Containment
Analysis and containment of damage

←

Recovery
Eradication of malware and back doors

←

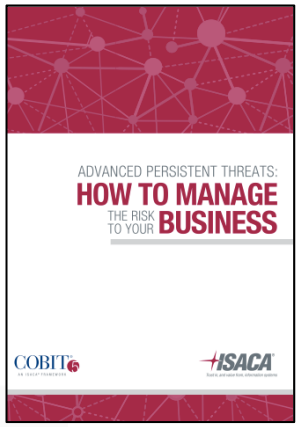
Investigation
Investigation of attacker, motives and impact

↓

Lessons Learned
Root cause analysis of contributing factors

→

***Post Mortem* Report**
Presenting findings to management

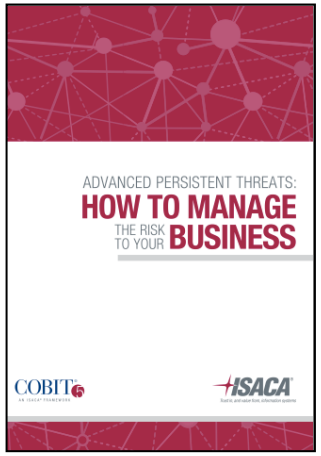


Cybersecurity goals

vital interacts

Increase attacker effort and cost

- Encryption, strong authentication, network segregation, layered filtering (application firewalls), data leak prevention
- Awareness and skills development
- Avoidance (e.g. don't collect and store data you don't need)
- Offensive security (e.g. honeypots; false ports, services and systems; web bugs/beacons)



Reduce gap between intrusion, detection and response

- Increase awareness of social engineering risks
- Implement inspection, event correlation and reporting systems and processes
- Increase incident response capabilities

vital interacts

CYBERSECURITY ASSURANCE

Audit and assurance guidance

vital interacts

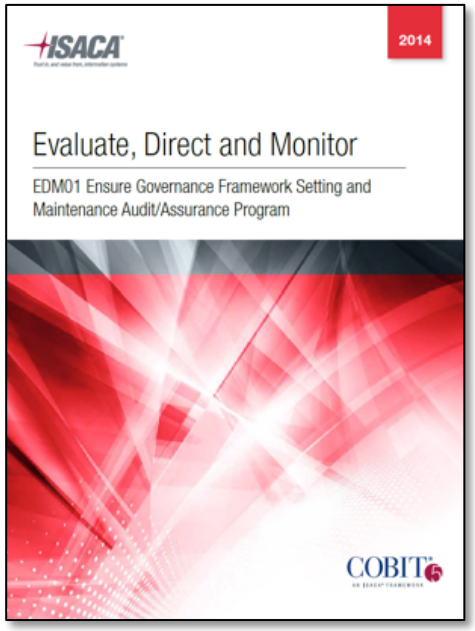
Audit / Assurance program guides cover:

- Evaluate, Direct and Monitor
- Align, Plan and Organise
- Build, Acquire and Implement
- Deliver, Service and Support

Aligned with generally accepted auditing standards and practices

Three phases:

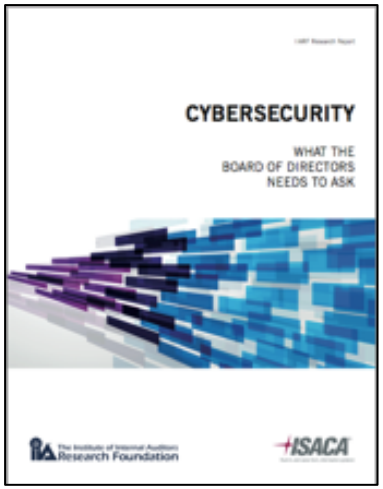
- Phase A: Determine scope
- Phase B: Understand enablers, set assessment criteria and perform the assessment
- Phase C: Communicate and report the results

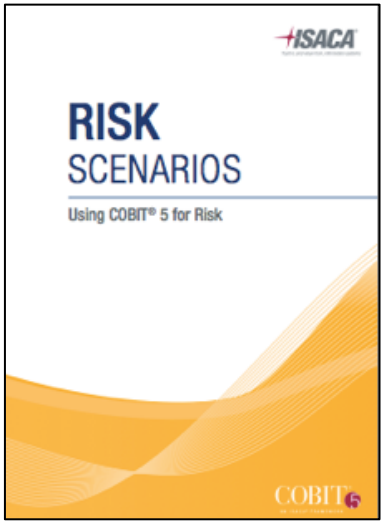


http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx

ISACA guidance

vital interacts



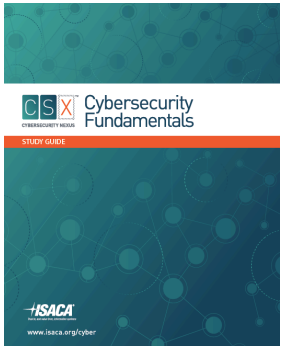


Assurance practices

vital interacts

Vulnerability management

"an exploitable weakness that results in a loss"



Vulnerability scanning

- Tool based scan of components for known vulnerabilities

Vulnerability assessment

- Analysis to identify vulnerabilities to assist risk and threat assessment of loss potential
- May be:
  - Technical
  - Procedural
  - Organisational
  - Emergent

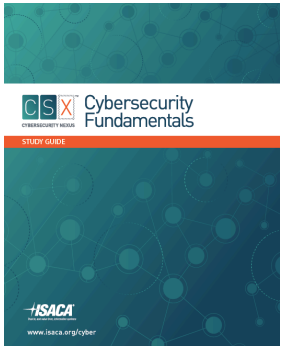
Assurance practices

vital interacts

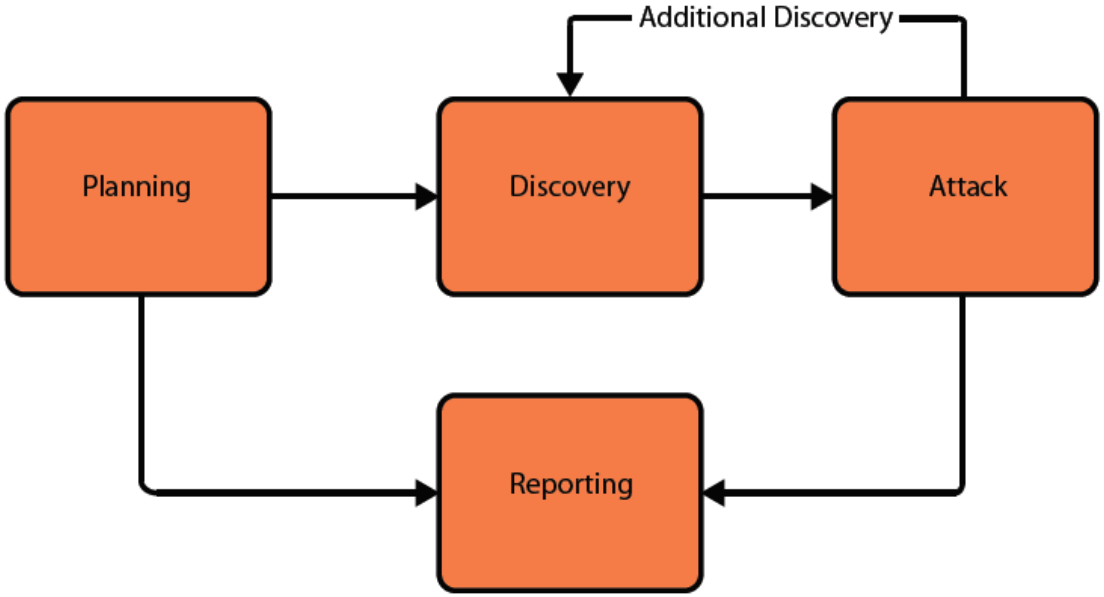
Penetration testing and code review

Identifying vulnerabilities and testing to confirm:

- if exploitable
- existence and effectiveness of controls
- potential exposure of assets



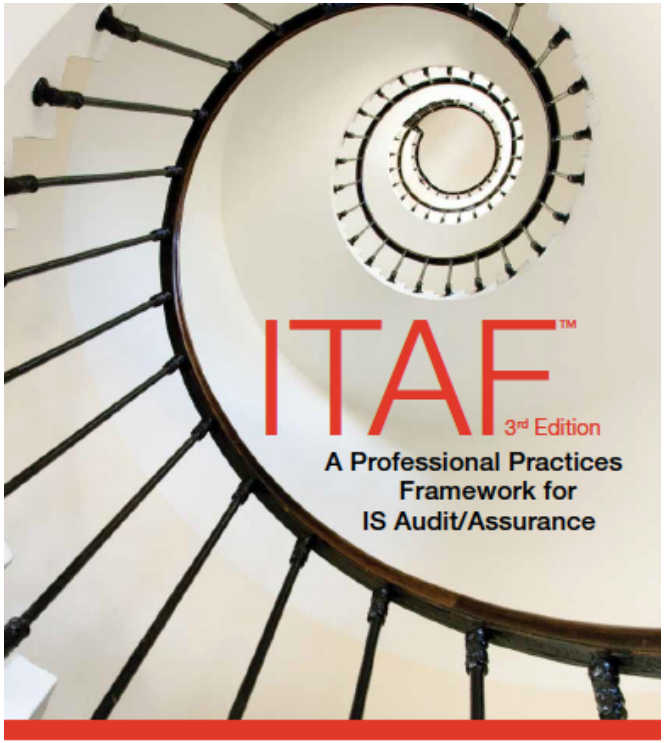
Phases of penetration testing



IT Audit Assurance Framework

vital interacts

Table of Contents



ISACA

vital interacts

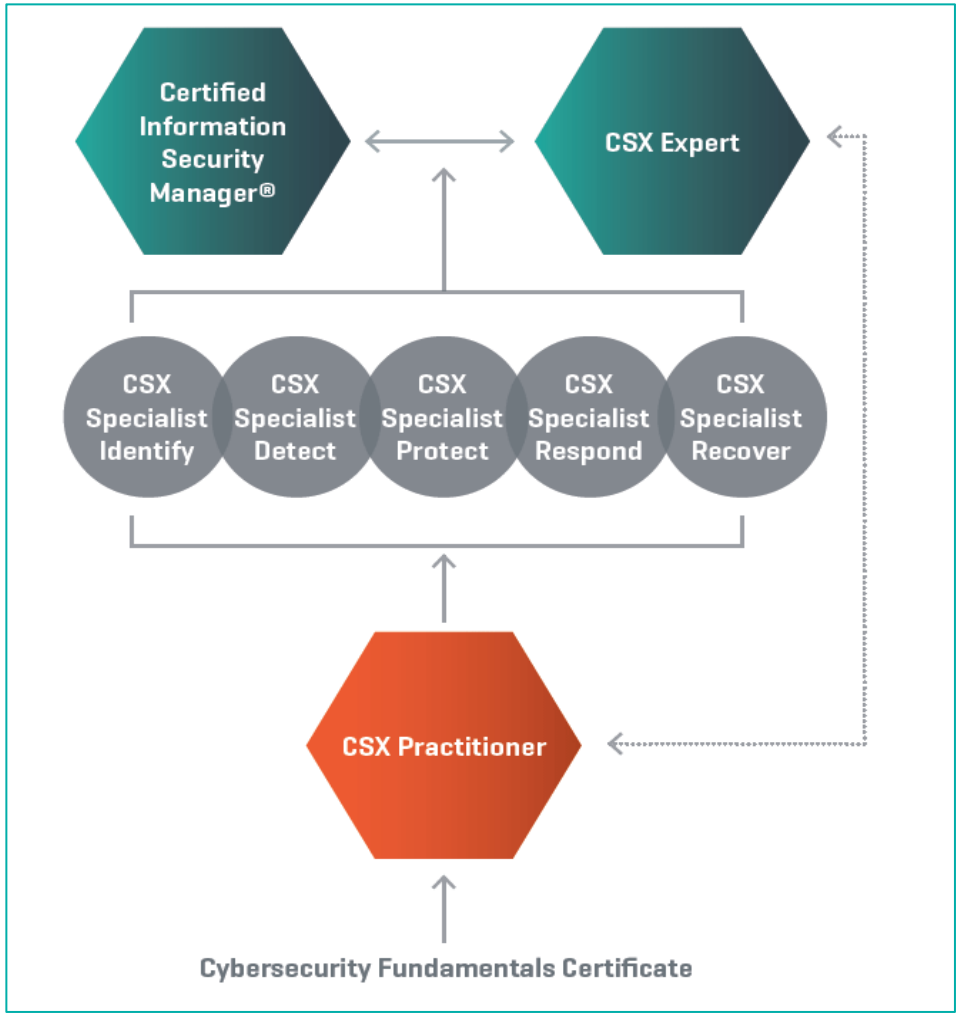
CYBERSECURITY SKILLS ISACA'S CSX

Cybersecurity Training and Certifications

CSX CERTIFICATIONS

CSX training and certifications will be offered for all skill levels and specialties throughout a professional's career.

https://cybersecurity.isaca.org/csx-certifications



Cybersecurity Training and Certifications

CSX Practitioner—Demonstrates ability to serve as a first responder to a cybersecurity incident following established procedures and defined processes. (1 certification, 3 training courses; prerequisite for CSX Specialist). Available now.

CSX Specialist—Demonstrates effective skills and deep knowledge in one or more of the five areas based closely on the NIST Cybersecurity Framework: Identify, Detect, Protect, Respond and Recover. (5 certifications, 5 training courses; requires CSX Practitioner). Available in 2016.

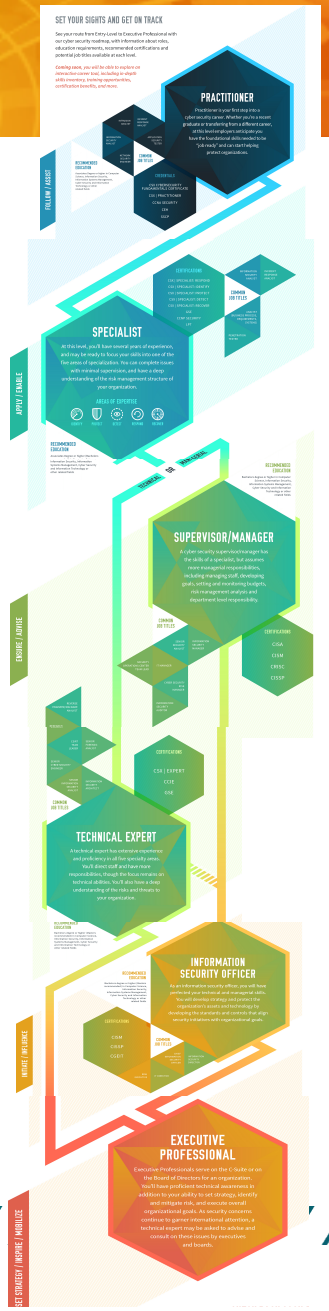
CSX Expert—Demonstrates ability of a master/expert-level cybersecurity professional who can identify, analyze, respond to and mitigate complex cybersecurity incidents. (1 certification, 1 training course; no prerequisites required). Available in 2016.

Certified Information Security Manager certification (26,000+ professionals certified since inception; named the highest-paying certification in Certification Magazine's 2015 Salary Survey.

Cybersecurity career roadmap

CSX provides you with the resources to continuously hone your skills, expand your knowledge, and start (and keep) your career on a trajectory toward achieving your goals.

https://cybersecurity.isaca.org/csx-careers



SET YOUR SIGHTS AND GET ON TRACK

See your route from Entry-Level to Executive Professional with our cyber security roadmap, with information about roles, education requirements, recommended certifications and potential job titles available at each level.

***Coming soon**, you will be able to explore an interactive career tool, including in-depth skills inventory, training opportunities, certification benefits, and more.*

FOLLOW / ASSIST

PRACTITIONER

Practitioner is your first step into a cyber security career. Whether you're a recent graduate or transferring from a different career, at this level employers anticipate you have the foundational skills needed to be "job ready" and can start helping protect organizations.

RECOMMENDED EDUCATION

Associates Degree or higher in Computer Science, Information Security, Information Systems Management, Cyber Security and Information Technology or other related fields

COMMON JOB TITLES

- INTRUSION ANALYST
- INCIDENT RESPONSE ANALYST
- INFORMATION SECURITY ANALYST
- APPLICATION SECURITY TESTER
- NETWORK SECURITY ENGINEER

CREDENTIALS

- CSX CYBERSECURITY FUNDAMENTALS CERTIFICATE
- CSX | PRACTITIONER
- CCNA SECURITY
- CEH
- SSCP

https://cybersecurity.isaca.org/csx-careers

APPLY / ENABLE

SPECIALIST

At this level, you'll have several years of experience, and may be ready to focus your skills into one of the five areas of specialization. You can complete issues with minimal supervision, and have a deep understanding of the risk management structure of your organization.

AREAS OF EXPERTISE

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

RECOMMENDED EDUCATION

Associates Degree or higher (Bachelors recommended) in Computer Science, Information Security, Information Systems Management, Cyber Security and Information Technology or other related fields.

CERTIFICATIONS

CSX | SPECIALIST: RESPOND
CSX | SPECIALIST: IDENTIFY
CSX | SPECIALIST: PROTECT
CSX | SPECIALIST: DETECT
CSX | SPECIALIST: RECOVER
GSE
CCNP SECURITY
LPT

COMMON JOB TITLES

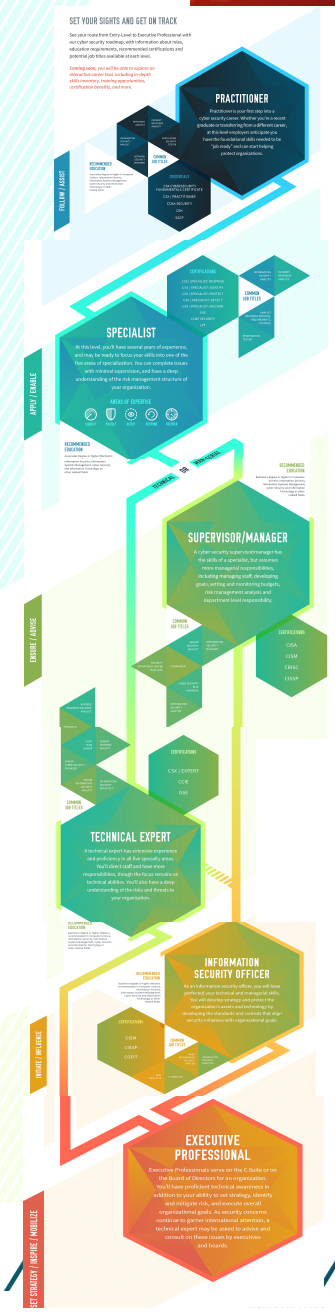
INFORMATION SECURITY ANALYST
INCIDENT RESPONSE ANALYST
ANALYST (BUSINESS PROCESS, REQUIREMENTS, SYSTEMS)
PENETRATION TESTER

MANAGERIAL

OR

RECOMMENDED EDUCATION

https://cybersecurity.isaca.org/csx-careers



Information Security, Information Systems Management, Cyber Security and Information Technology or other related fields

TECHNICAL OR MAN

RECOMMENDED EDUCATION

Bachelors degree or higher in Computer Science, Information Security, Information Systems Management, Cyber Security and Information Technology or other related fields

SUPERVISOR/MANAGER

A cyber security supervisor/manager has the skills of a specialist, but assumes more managerial responsibilities, including managing staff, developing goals, setting and monitoring budgets, risk management analysis and department level responsibility.

ENSURE / ADVISE

COMMON JOB TITLES

SENIOR SECURITY ANALYST

INFORMATION SECURITY MANAGER

SECURITY OPERATIONS CENTER TEAM LEAD

IT MANAGER

CYBER SECURITY RISK MANAGER

INFORMATION SECURITY AUDITOR

REVERSE ENGINEER/MALWARE ANALYST

RESEARCH ENGINEER

CERTIFICATIONS

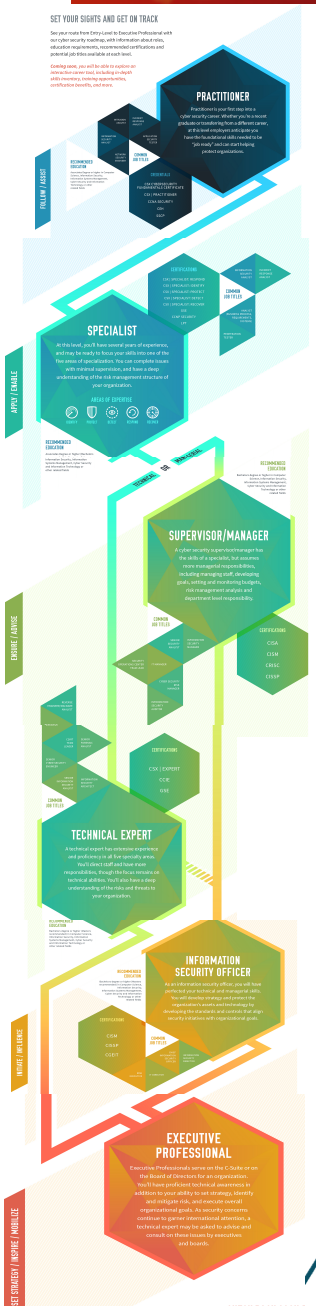
CISA

CISM

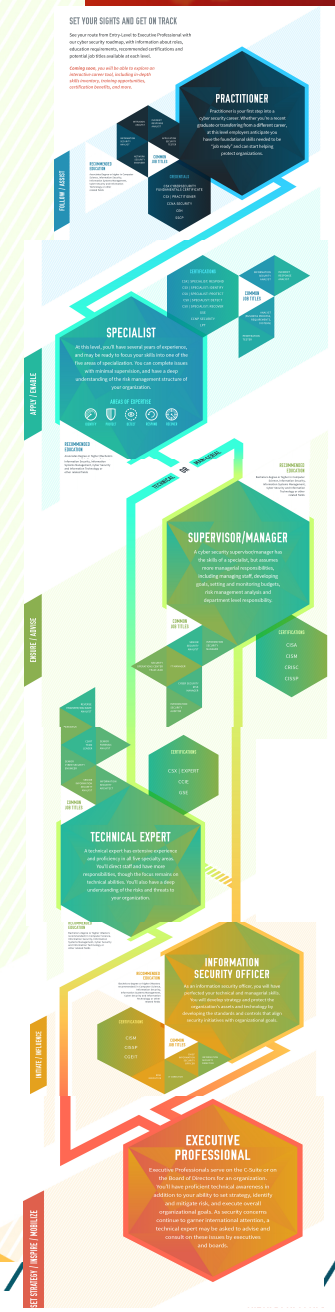
CRISC

CISSP

https://cybersecurity.isaca.org/csx-careers



https://cybersecurity.isaca.org/csx-careers



RECOMMENDED EDUCATION

Bachelors degree or higher (Masters recommended) in Computer Science, Information Security, Information Systems Management, Cyber Security and Information Technology or other related fields

INFORMATION SECURITY OFFICER

As an information security officer, you will have perfected your technical and managerial skills. You will develop strategy and protect the organization's assets and technology by developing the standards and controls that align security initiatives with organizational goals.

RECOMMENDED EDUCATION

Bachelors degree or higher (Masters recommended) in Computer Science, Information Security, Information Systems Management, Cyber Security and Information Technology or other related fields

CERTIFICATIONS

CISM

CISSP

CGEIT

COMMON JOB TITLES

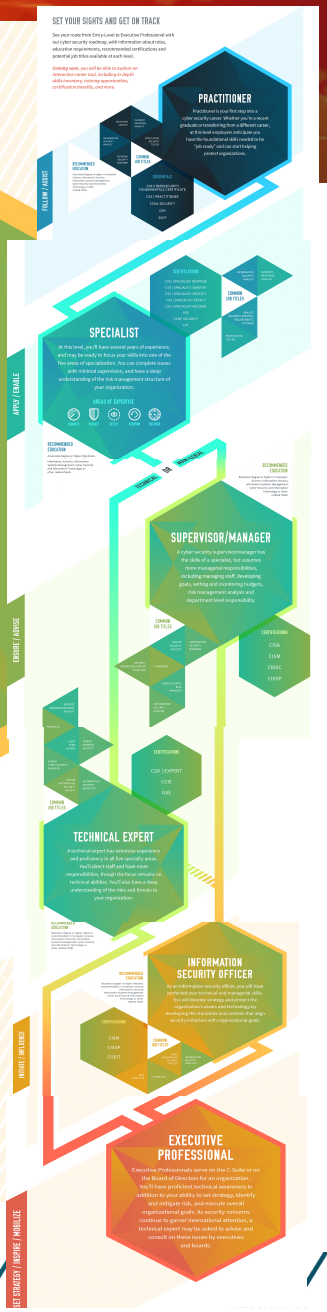
CHIEF INFORMATION SECURITY OFFICER

INFORMATION SECURITY DIRECTOR

RISK EXECUTIVE

IT DIRECTOR

INITIATE / INFLUENCE



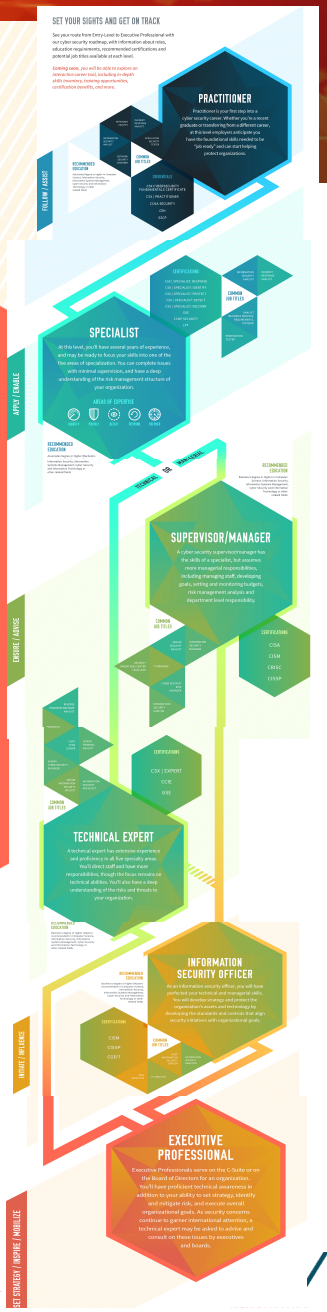
https://cybersecurity.isaca.org/csx-careers

EXECUTIVE PROFESSIONAL

Executive Professionals serve on the C-Suite or on the Board of Directors for an organization. You'll have proficient technical awareness in addition to your ability to set strategy, identify and mitigate risk, and execute overall organizational goals. As security concerns continue to garner international attention, a technical expert may be asked to advise and consult on these issues by executives and boards.

SET STRATEGY / INSPIRE / MOBILIZE

https://cybersecurity.isaca.org/csx-careers

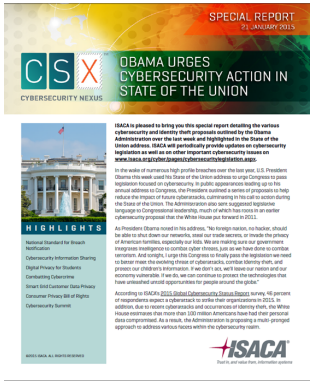


CSX resources and tools

- Cybersecurity Guidance for Small and Medium-Sized Enterprises
- Implementation guides for NIST Cybersecurity Framework and EU cybersecurity guidance
- 2015 APT study
- CSX Cybersecurity Legislation Watch

UPCOMING ELEMENTS:

- Career management road map
- Threats and controls tool
- CSX Specialist and CSX Expert certifications



CSX 2016 Events

- **Asia: Singapore**
- **Europe: London, UK**
- **North America: Las Vegas, Nevada, USA**

CSX™ 2016 NORTH AMERICA
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

www.isaca.org/cyber-con

Open discussion

vital interacts

What are the key cybersecurity challenges facing Fiji?

What are the implications for government, business and the people of Fiji?

What practical steps can be taken now to resolve these?

EuroCACS Cyber panel observations:

vital interacts

Security is becoming more and more difficult

There are not enough people to do this work

Technology change is happening faster and faster

The bad guys are becoming more diverse and are innovating at an increasing rate and include new dimensions such as cyber terrorism

Small and medium sized businesses generally cannot assert security as a core competency for their business (much like they can't do it for HR, audit, compliance, legal and other specializations)

Large businesses and governments want to offload commodity services and benefit from "shared spaces"

The cloud and service providers offer an opportunity to aggregate security core competencies across a range of disciplines (advanced threat management, IR, intel, GRC, authentication, etc.) and also benefit from the power of aggregated security information and intelligence management

vital interacts

QUESTIONS

Thank you for your contributions

garry.barnes@vitalinteracts.com