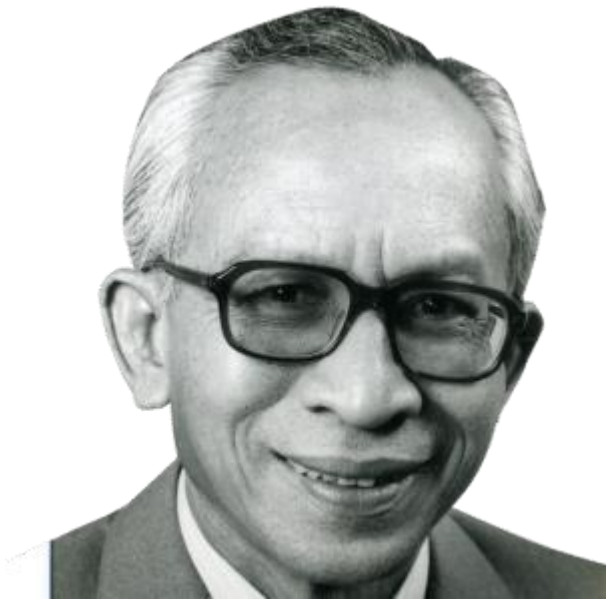
CSX™
CYBERSECURITY NEXUS

CHALLENGES IN AUDITING: CYBER THREAT AND TECHNOLOGY

KENNETH HO, CISA, CISM, CGEIT
26 OCTOBER 2017

ISACA®
Trust in, and value from, information systems
Malaysia Chapter

Introduction – Who are we?



ISACA®

Trust in, and value from, information systems

Malaysia Chapter

ISACA Malaysia Chapter was established way back in November 1984. Our first President was none other than the Auditor General himself at that time, the Honorable Late Tan Sri Ahmad Noordin bin Hj Zakaria.

A nonprofit, independent membership association, ISACA helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the nonprofit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification.

ISACA – In a nutshell

ISACA Facts and Figures

Established: 1969
Engaged Professionals: More than 520,000
Members: More than 130,000 in 188 countries
Members and Certification-Holders: More than 159,000
Chapters: More than 215
Student Groups: More than 80

ISACA Certifications

ISACA developed and administers industry-leading certifications:

Certified Information Systems Auditor® (CISA®).More than **130,000** CISAs have been certified since its inception in 1978.

Certified Information Security Manager® (CISM®). More than **34,000** CISMs have been certified since 2002.

Certified in the Governance of Enterprise IT® (CGEIT®). More than **7,000** CGEITs have been certified since 2007.

Certified in Risk and Information Systems Control™ (CRISC™). More than **20,000** CRISCs have been certified since 2010.

CSX Practitioner Certification (CSXP™) is a performance-based certification allowing practitioners to validate their skills as a cyber security first-responder.

Defining Cybersecurity

- **Information Security**

Preservation of Confidentiality, Integrity and Availability of **information**; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

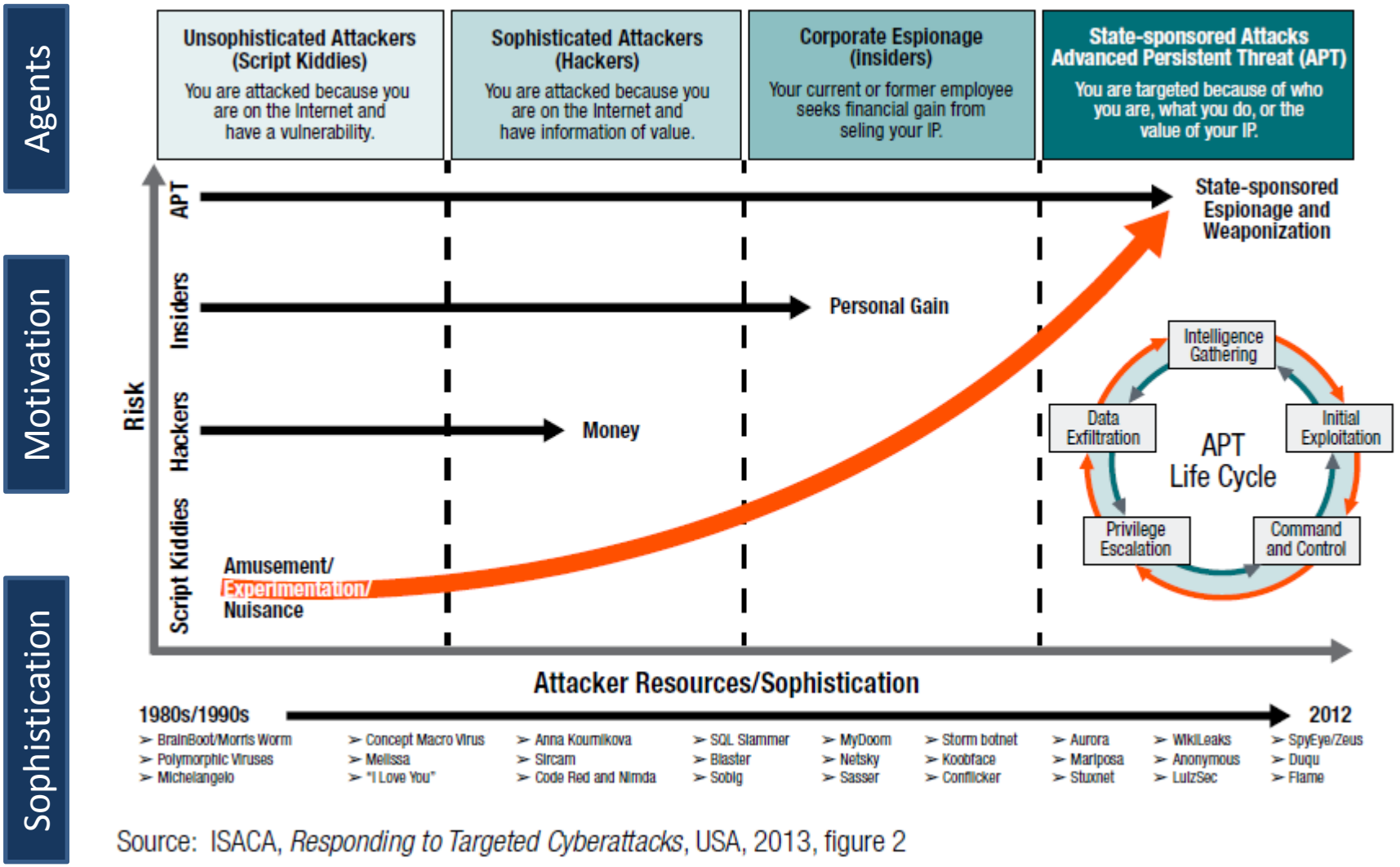
Source: ISO27000

- **Cybersecurity**

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

Source: ISACA

Evolution of Threat Landscape

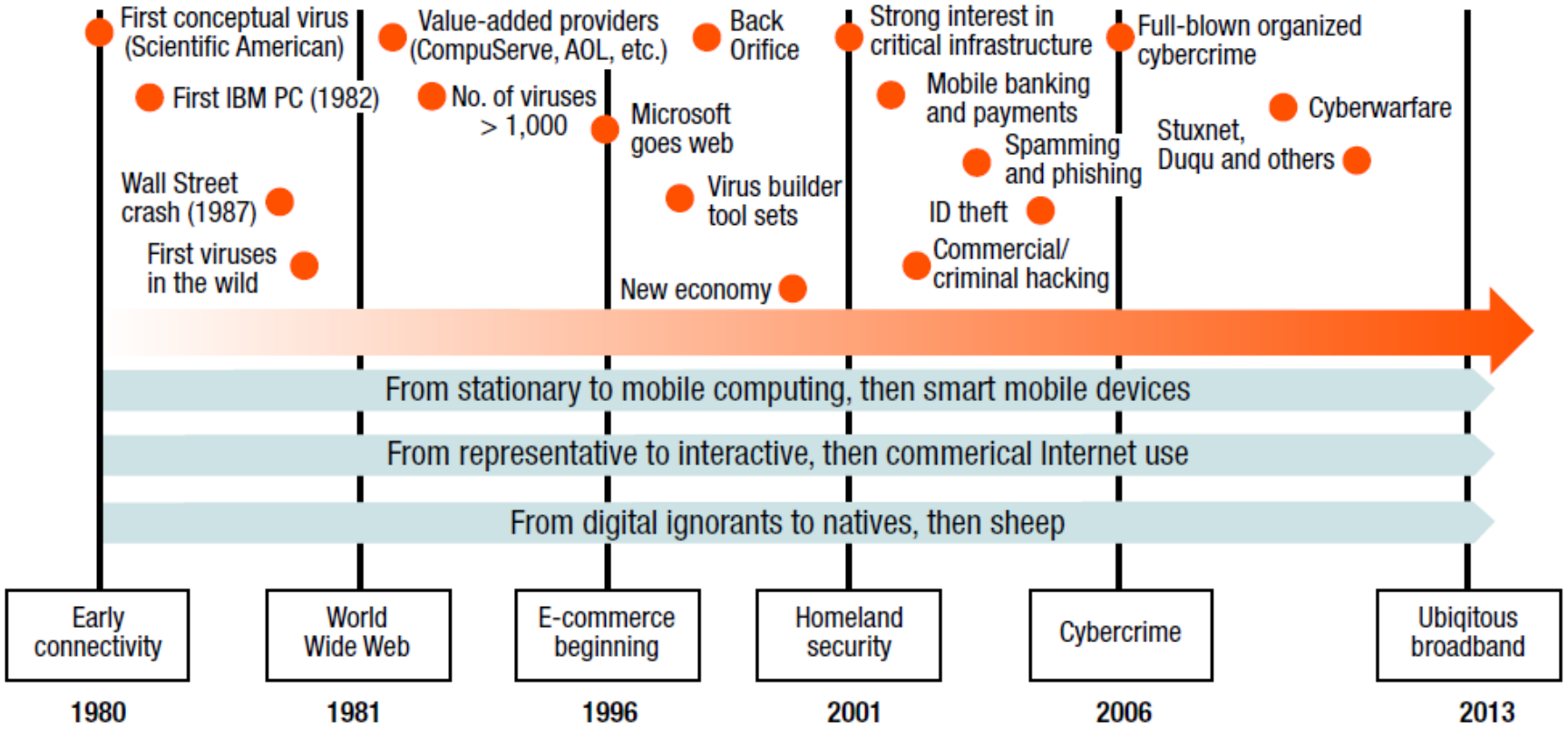


Source: ISACA, *Responding to Targeted Cyberattacks*, USA, 2013, figure 2

Source: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Responding-to-Targeted-Cyberattacks.aspx

ISACA Malaysia Chapter

Cybersecurity Timeline

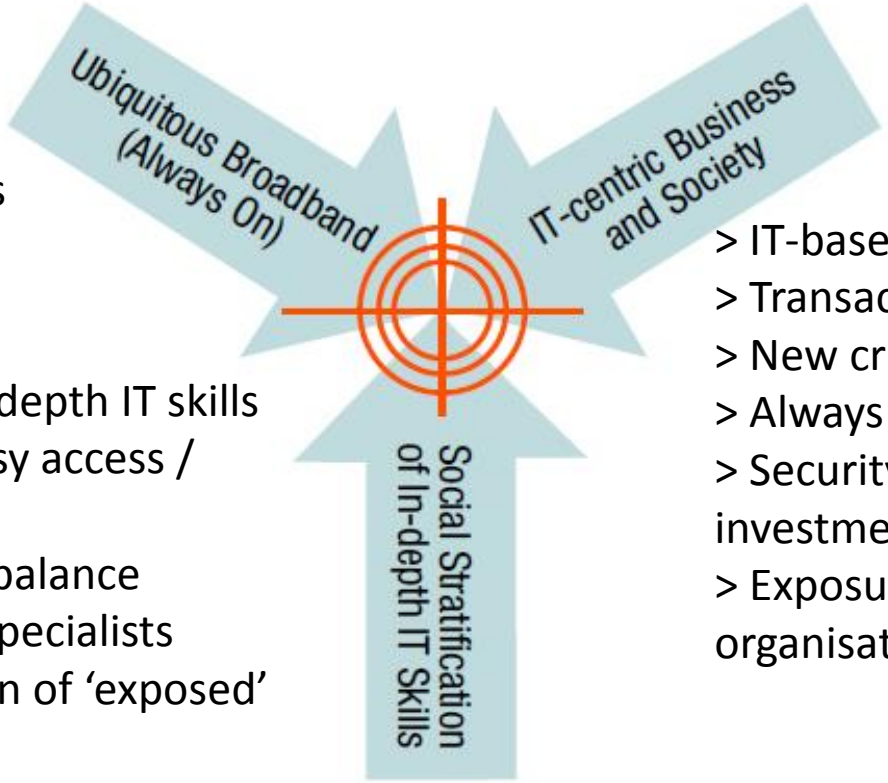


Source: von Roessing, Rolf M., 2012

Source: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/transforming-cybersecurity-using-cobit-5.aspx

What are the recent game changer?

> Cloud
> Public access points
> Traveling user exposure
> Opportunity for attack
< Time required for attacks
>> Range of services



> IT-based transactions
> Transaction value
> New critical infrastructure
> Always on social media
> Security demands – higher investments
> Exposure for attack for organisations & individuals

< 'People' with in-depth IT skills
> 'People' with easy access / convenience
>< Educational imbalance leading to less IT specialists
> Larger proportion of 'exposed' individuals
> Growing educational gap as systems favours convenience over user controls

Source: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/transforming-cybersecurity-using-cobit-5.aspx

Current Threat Landscape of 2015 vs 2016

ENISA Threat Landscape Report 2016
Final version | 1.0 | OPSEC | January 2017

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	→	6. Phishing	→	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	→	8. Ransomware	→	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	→	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	→	11. Exploit kits	↑	↓
12. Identity theft	→	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2016 with the one of 2015[1].

Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Cybersecurity Threat Moving Forward

Cyber security experts expect cyber security threats to continue in 2017, with innovative attacks. Cyber crime is profitable and the risks for the criminals to be caught or punished are still negligible. 2017 is likely to see more copycat crimes as well as increased sophistication in attacks.

1. Malware
2. Social Engineering
3. Internet of Things
4. Insider
5. Cyber Espionage
6. Access Control
7. BYOD
8. Web-Based Infection and Browser-Based Exploits
9. Flaws in Widely-Used Open Source Software
10. Watering Hole

Source: http://www.cyber-securitygroup.net/2015-small-business-cyber-security-threats/

Protection for Business

Protection for Business (continued)

Basic Security Measures

- Antivirus systems (signature or heuristics)
- Intrusion Detection Systems
- Firewalls
- Penetration Testing
- Strong Authentication (physical token, smart card etc)

Advanced Security Measures

- Intrusion Prevention Systems
- Data Leak Prevention
- Vulnerability Scanning
- Penetration Testing
- Database Activity Monitoring (DAM)
- Application Security Testing

Protection for Business (continued)

Specific Advance Threat Countermeasures

- Advance Endpoint Protection
- Network Packet Inspection
- Advance Persistent Threat Detection (“APT”)
- Distributed Denial of Services (“DDOS”)
- File Integrity Monitoring (“FIM”)
- Security Information and Event Management (“SIEM”)
- Indicator Of Compromise Assessment (“IOC”)

Best Available Security Practices

- Security Development Lifecycle
- Disaster Recovery

Solutions to your problems?

Area	Threats	Solutions / Mitigation
External	DDoS, IoT	Akamai, Clean Pipe, WAF
	Website Hacking	Firewall/IPS/IDS, server hardening, code review, penetration testing
	Virus and Malware	Anti-virus, anti-malware, firewall, proxy server, spam filter
Internal	Data Leakage	Policies, APT, DLP, MDM
	Data Leakage (IT)	PVM, FIM
	Ignorance	Education, Awareness Training, policies
Operation	Crisis	SIEM, SOC, Cyberdrill
	The Unknown	APT, GTI

Start from the Basics - NIST Cybersecurity Framework

- Developed by the National Institute of Standards and Technology, issued in February 12, 2014 (under revision now for version 2017).
- Covers 5 domains which includes the following:

Areas	Descriptions
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.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Source: https://www.nist.gov/cyberframework

14

IS Audit/Assurance Program for Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program

In light of the increasing volume and sophistication of cyberattacks, ISACA has developed an audit/assurance program based on the NIST Cybersecurity Framework to provide organizations with a formal, repeatable way to evaluate cybersecurity controls.

The objective of a cybersecurity audit is to provide management with an evaluation of the **effectiveness of cybersecurity processes, policies, procedures, governance and other controls**. The review will focus on cybersecurity standards, guidelines and procedures as well as the implementation of these controls.

The audit/assurance review will **rely upon other operational audit**s of the incident management process, configuration management and security of networks and servers, security management and awareness, business continuity management, information security management, governance and management practices of both IT and the business units, and relationships with third parties.

The primary security and control issues include:

- **Protection of sensitive data** and intellectual property
- **Protection of networks** to which multiple information resources are connected
- **Responsibility and accountability** for the device and information contained on it

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

15

IS Audit/Assurance Program for Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program

Audit Objectives

- Provide management with an **assessment** of their cybersecurity **policies and procedures** and their **operating effectiveness**.
- Identify **security control** concerns that could affect the **reliability, accuracy and security** of the enterprise data due to weaknesses in security controls.
- Evaluate the **effectiveness of response and recovery** programs.

Audit Scope

The audit/assurance program is built on the following five critical cybersecurity activities:

- Identify
- Protect
- Detect
- Respond
- Recover

The auditor conducting the audit will identify **the scope of organizational systems and assets** to be reviewed.

The audit/assurance program can be adapted to support various business processes, applications or systems with **different security requirements**.

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

16

IS Audit/Assurance Program for Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program

Minimum Audit Skills

The IT audit and assurance professional must have an **understanding of security and controls**. Because this is a dynamic field, professionals performing this audit should ensure that they have performed the **necessary research to understand the underlying technologies used in cybersecurity** to identify, protect, detect and respond to cyberthreats and attacks. However, it is important that the auditor has **sufficient functional and business knowledge** to assess alignment with the business strategy.

Professionals holding the CISA certification should comply with ITAF standard 1006 Proficiency.

- ❑ General standards (1000 series)
- ❑ Performance standards (1200 series)
- ❑ Reporting standards (1400 series)—Address the types of reports, divided into three categories: -
  - ✓ General guidelines (2000 series)
  - ✓ Performance guidelines (2200 series)
  - ✓ Reporting guidelines (2400 series)

Testing Steps

Audit steps have been developed for each NIST Cybersecurity Framework subcategory to evaluate the effectiveness of the organization's controls. Refer to the Cybersecurity NIST **Audit Program Excel spreadsheet** for the full audit/assurance program.

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

17

NIST Cybersecurity Framework Audit Program - Identify

Process Sub-Area	Control Objectives	Controls
Asset Management	The **data, personnel, devices, systems, and facilities** that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Physical devices and systems within the organization are inventoried.
		Software platforms and applications within the organization are inventoried.
		Organizational communication and data flows are mapped.
		External information systems are cataloged.
		Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality and business value.
		Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	The organization's role in the supply chain is identified and communicated.
		The organization's place in critical infrastructure and its industry sector is identified and communicated.
		Priorities for organizational mission, objectives and activities are established and communicated.
		Dependencies and critical functions for delivery of critical services are established.
		Resilience requirements to support delivery of critical services are established.
Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Organizational information security policy is established.
		Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.
		Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
		Governance and risk management processes address cybersecurity risk.

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

NIST Cybersecurity Framework Audit Program - Protect

Process Sub-Area	Control Objectives	Controls
Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Identities and credentials are managed for authorized devices and users.
		Physical access to assets is managed and protected.
		Remote access is managed.
		Access permissions are managed, incorporating the principles of least privilege and separation of duties.
		Network integrity is protected, incorporating network segregation where appropriate.
Awareness Training	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	All users are informed and trained.
		Privileged users understand roles and responsibilities.
		Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities.
		Senior executives understand roles and responsibilities.
		Physical and information security personnel understand roles and responsibilities.

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

NIST Cybersecurity Framework Audit Program - Detect

Process Sub-Area	Control Objectives	Controls
Anomalies and Events	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	A baseline of network operations and expected data flows for users and systems is established and managed.
		Detected events are analyzed to understand attack targets and methods.
		Event data are aggregated and correlated from multiple sources and sensors.
		Impact of events is determined.
		Incident alert thresholds are established.
Security Continuous Monitoring	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	The network is monitored to detect potential cybersecurity events.
		The physical environment is monitored to detect potential cybersecurity events.
		Personnel activity is monitored to detect potential cybersecurity events.
		Malicious code is detected.
		Unauthorized mobile code is detected.
		External service provider activity is monitored to detect potential cybersecurity events.
		Monitoring for unauthorized personnel, connections, devices and software is performed.
		Vulnerability scans are performed.

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

NIST Cybersecurity Framework Audit Program - Respond

Process Sub-Area	Control Objectives	Controls
Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	Response plan is executed during or after an event.
Communications	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	Personnel know their roles and order of operations when a response is needed.
		Events are reported consistent with established criteria.
		Information is shared consistent with response plans.
		Coordination with stakeholders occurs consistent with response plans.
		Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Analysis	Analysis is conducted to ensure adequate response and support recovery activities.	Notifications from detection systems are investigated.
		The impact of the incident is understood.
		Forensics are performed.
		Incidents are categorized consistent with response plans.

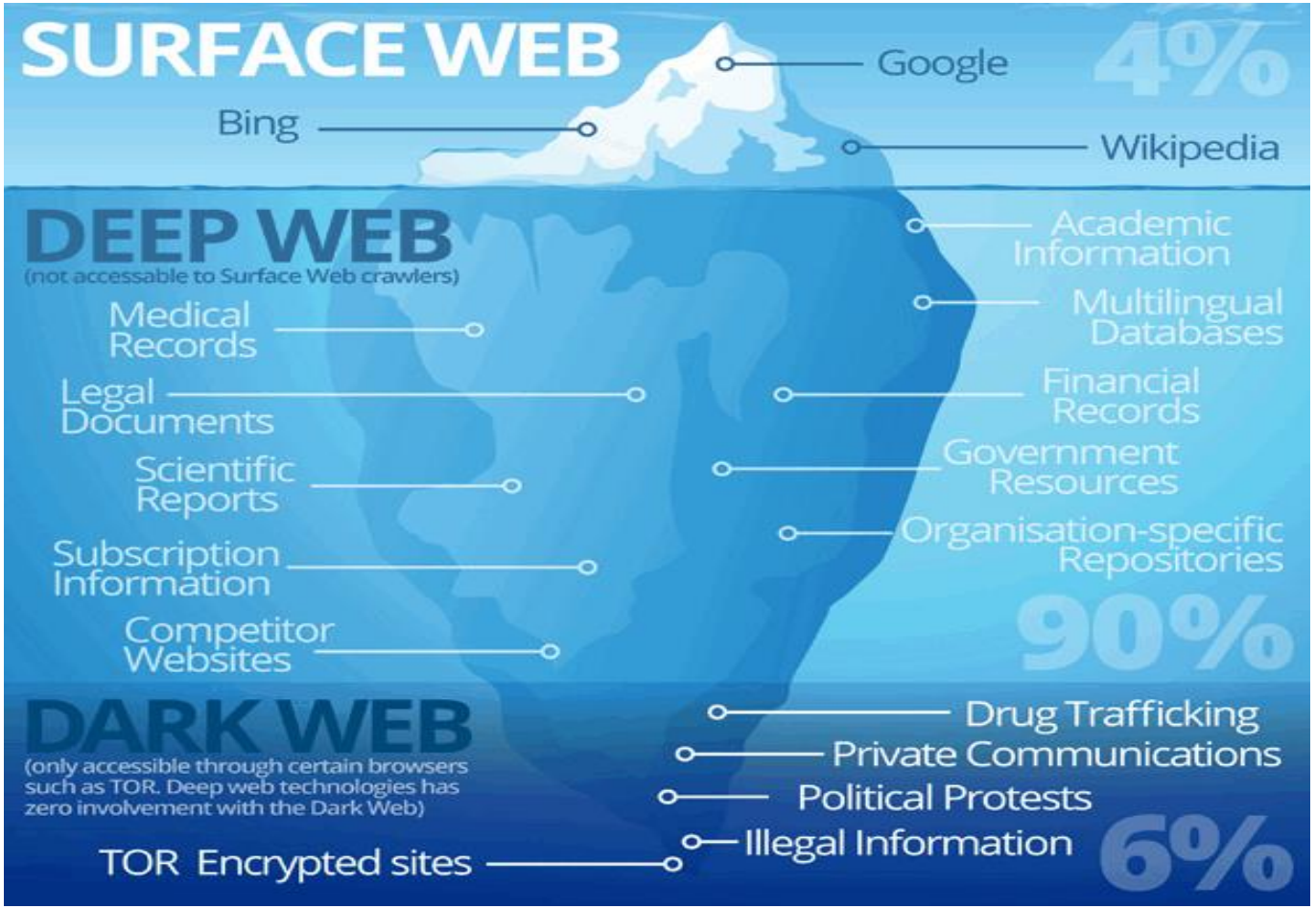
Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

NIST Cybersecurity Framework Audit Program - Recover

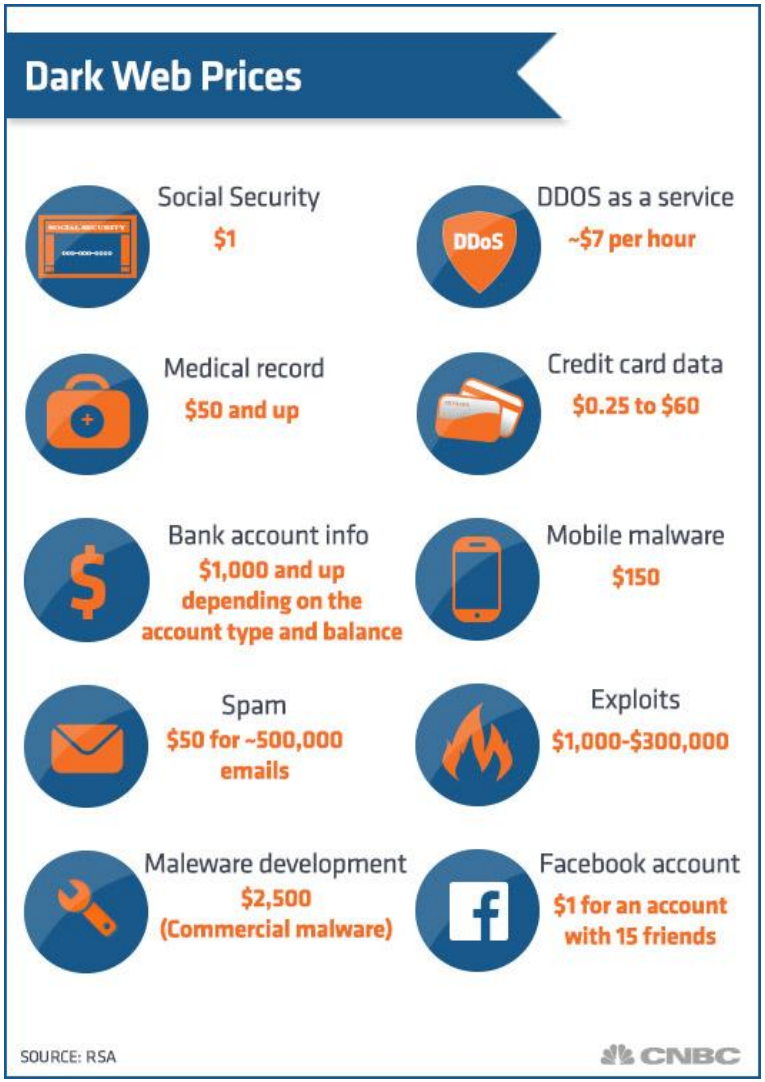
Process Sub-Area	Control Objectives	Controls
Recovery Planning	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	Recovery plan is executed during or after an event.
Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned.
		Recovery strategies are updated.
Communications	Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs and vendors.	Public relations are managed.
		Reputation after an event is repaired.
		Recovery activities are communicated to internal stakeholders and executive and management teams.

Source: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx?cid=pr_1208731&appeal=pr

Yes, the Dark Web does exists….



Dark Web Prices…..



Source: https://www.cnbc.com/2014/10/03/hackers-selling-stolen-card-info-online-thats-the-least-of-it.html

Summary

- Cybersecurity is complex and its risk is real.
- Cybersecurity is costly but failing to act could be worse. It's always a balance between risk and cost.
- Start with the basics, conduct risk assessment on cyber threats, seek management buy-in, invest on advanced security technologies, educate your users, recruit cyber specialist and have a good incident management procedure in hand.
- Cybersecurity is not just an IT problem, it cuts across the organisation and it will affect everyone including Internal Auditors.
- Cybersecurity is real. Deal with it. It is just a matter of time before your organisation will be targeted.

Thank You!

Appendix 1 - Acronyms

Short name	Description
DDoS	Distributed Denial of Service
APT	Advanced Persistent Threat
DLP	Data Loss Prevention
MDM	Mobile Device Management
FIM	File Integrity Management
CM	Change Management
PVM	Password Vault Management
SIEM	Security Incidents and Events Management
SOC	Security Operations Centre
GTI	Global Threat Intelligence