DREW & NAPIER

Cybersecurity 101: Trends and Best Practices

13 May 2020

Albert Pichlmaier
Senior Cybersecurity Engineer , Data Protection, Privacy & Cybersecurity

AGENDA & Learning points

1. Security Fundamentals & Best Practices
   - ✓ Understand the need for consistent terminology
   - ✓ Differentiate different disciplines around security & DP
   - ✓ Utilise the common fundamental principles of security
   - ✓ Identify the types of security issues and how hackers use them
   - ✓ Appreciate the complexity of secure implementation based on two frequently misunderstood best practices

2. Trends
   - ✓ Understand scope of ISO/IEC 27701, and beware of certification limitations
   - ✓ Recent threat landscape

Part I : Fundamentals & Best Practices

DREW & NAPIER

Security – Hindrance or Enabler?

- Security is about making it harder for the attacker (not user)
  - E.g. Brute force is always possible, so use counter, time, longer key etc.
- Security is about making things easier and more convenient for users
  - E.g. ATM, Internet and Mobile banking, SIM cards, IoT
- Security is about making new things work for organisations
  - E.g. Anonymisation techniques and data sharing frameworks allow for extended services with reduced risk

DREW & NAPIER

Terminology & Clarity – Key for security

Customer: "*Do you have a four Volt, two Watt light bulb?*"

Salesman: "*For what?*"

Customer: "*No, two.*"

Salesman: "*To what...*"

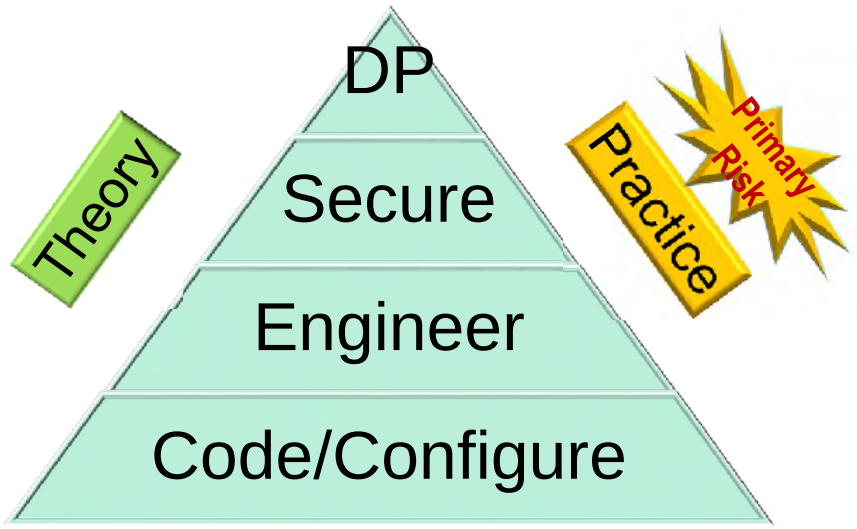
Customer: "*Yes.*"

Salesman: "*No*"

If you hear '*We are secure(d)!*',
ask '*Against or for what?*'

Just as there is no fail-proof terminology, there is no single and practical 100% security – in other words: it's all about 'risk'

Security and DP: 'something extra'



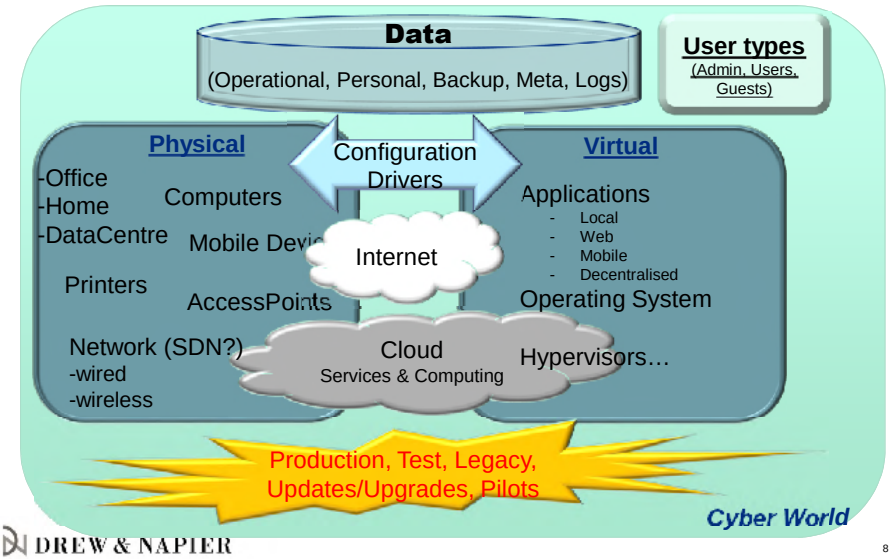
What is (IT, cyber, computer, info...) Security?

- Core information security fundamentals (data & systems) are:
  - **Confidentiality** Prevent unauthorized use/disclosure
  - **Integrity** Process correctly and detect/prevent modification
  - **Availability** Provide reliable (timely/proper/intended) processing

- Extended with:
  - **Non-repudiation** Prevent denial of action (mostly sender side)

- Associated with IAAAA (information system and access management)
  - **Identification** Unique reference within a system
  - **Authentication** Verify/ascertain identity
  - **Authorization** Grant (and deny) permissions
  - **Accountability** Evidence for actions of entities, mostly users
  - **Audit** Recording of user/system events

Security needs to cover ... ***each*** and ***all*** *and more*



Security Domains (as per 2018 CISSP curriculum)

• Security and Risk Management	CIA, risk, policy & regulation
• Asset Security	Types, DP, controls, storage
• Security Architecture and Engineering	Security Model, secure design, crypto, physical security
• Communication and Network Security	Architecture, components, protocols, secure comms
• Identity and Access Management (IAM)	Access, IAM authorisation
• Security Assessment and Testing	Planning, execution, audit
• Security Operations	Investigation, operation, incident mgmt, DR, BCP
• Software Development Security	Lifecycle, implementation, threats, third party

DREW & NAPIER

9

Where do security problems actually arise?

- Issues versus Risk
  - Anomaly — indicates
  - Bug/Glitch — constitutes
  - Weakness — is taken advantage of
  - Vulnerability — may allow misuse via
  - Exploit — automated as kit/service

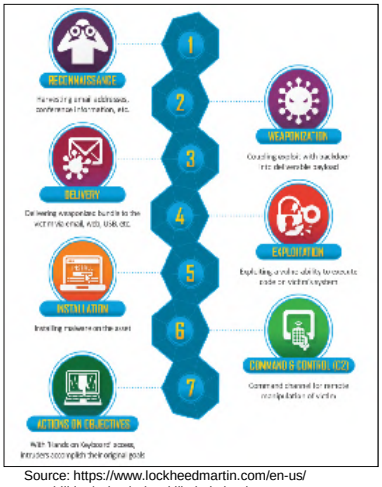
But all this is just theory if you don't even know what ***data assets*** you have, how it is used, and where it is… or what SW or devices there are, and where, and what they do…

- Risk versus Damage
  - 'Risk' — (not 'if' but 'when'), likelihood of occurrence
  - Exposure — feared event, potential to know/find vulnerability
  - Threat — potential (for mis-) use of vulnerability
  - Attack — manifest threat/exercise vulnerability
  - Compromise — successful attack and foothold
  - Breach — violation of system/policy and possibly regulation
  - 'Risk' — amount of impact

DREW & NAPIER

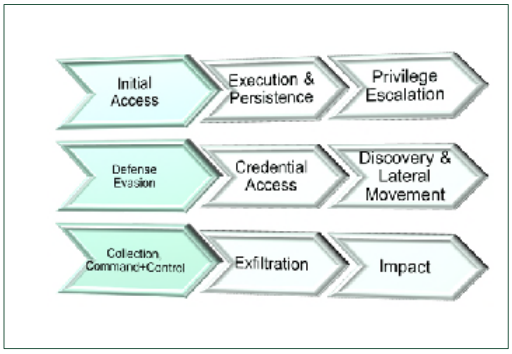
10

How do (external) attackers proceed?



Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Stages in a cyber attack



Based on : https://attack.mitre.org/resources/enterprise-introduction/ And www.ncsc.gov.uk/

Basic and 'advanced' authentication

- Passwords authenticate user-ID (not the user!):
  - 8 characters are strong (for *offline* users), only if unpredictable (no default PW is)
  - Many 2FA are from an attackers view NOT a 'what you have'
  - Brute force (both 1FA and 2FA) needs to be stopped:
    - Counter, time delay, etc: balance 'hard for attacker' and 'easy for user'
    - Continuous attack: repeat in between, attack over months
  - Beware: Is any delegated login an authentication or an authorisation token?
- Implementing a 'secure' (password and especially cryptographic) verification as part of the authentication process is not easy, especially in embedded systems
- Alternatives to passwords:
  - Auto-login tends to 'confuse/confound' Identification with Authentication
  - Biometrics tends to 'confuse/confound' Identification, Authentication *and* Authorisation (facial recognition is like announcing your password all over social networks, so the security is not in the facial recognition but the life detection)

Hiding data is not enough

- Signals/Requests like ‘Do not proceed’ (no-robot file)
  - – No security
- Encoding/Decoding (Morse, Base64)
  - – No security
- Hashing (salt, block-chain)
  - + One way function
  - + Low collision
- Encrypt/decrypt /sign
  - + Protects in terms of Confidentiality and Integrity
  - + Signer non-repudiation with asymmetric cryptography
  - ? Key creation
  - ? Key management
  - ? Type and amount of encrypted data

Part II : Trends

ISO 27000 Family

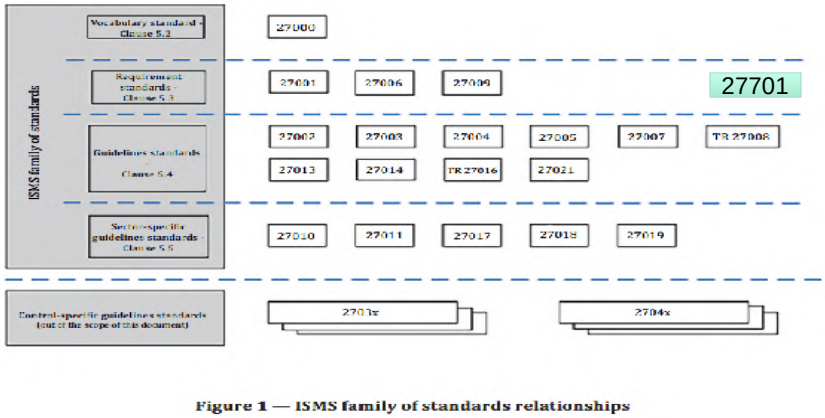


Figure 1 — ISMS family of standards relationships

* Source: ISO/IEC 27000:2018: ISMS — Overview and Vocabulary (is without ISO/IEC 27701; added to illustrate to which area it belongs) (freely available at https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html;)

ISO/IEC 27701:2019

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

- Specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a **Privacy Information Management System** (PIMS) in the form of **an extension** to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization
- Requirements and guidance can be applied to **PII controllers** and **PII processors**, holding responsibility and accountability for PII processing
- ISO/IEC 27001/27002 refers to 'information security', within ISO/IEC 27701 that needs to read 'information security and privacy'
- Aligns and extends ISO/IEC 27001/27002, but also refers to:
  - ISO 29100 *Information technology – Security techniques – Privacy framework*
  - ISO 29151 *Information technology – Security techniques – Code of practice for personally identifiable information protection*
  - ISO 27018 *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.

Basic Overview

- It targets to be a 'common denominator', mapping to GDPR
- Additional mappings exist outside the standard (demonstrated last year at IAPP)
- Mapping between the requirements needs interpretation according to the local law in order to fulfill the 27001 requirement to take local context into consideration, such that unique local regulatory requirements need to be spelt out and incorporated
- Extends 27001/2 in the following manner:
  - Existing elements remain as-is and are referenced
  - There are additional privacy-specific requirements/guidance
  - Addresses generic DP obligations as well

For summary and Table on Contents see https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

Certification & Recognition

- Despite its current status and some uncertainty in terms of application and legal compliance, it is a necessary and important, though still optional, extension for ISO/IEC 27001 certifications
- ISO/IEC 27701 is an *extension* to ISO/IEC 27001, and therefore is not separately certifiable (Note: certification is made against requirements, and not against controls, so there is no ISO/IEC 27002 certification)
- Certification assures compliance with the standard, it is not automatically compliance with a DP-law
- While a certification cannot prove compliance, it can prove an organisation's effort to work towards compliance
- Localisation requirements could raise concerns about international recognition of the 27701 part

Singapore context

- Certifications, seals and marks are encouraged by regulators. They may help to demonstrate compliance; but the extent to which they are accepted depends on the regulator.
  - ISO/IEC 27701 is not a replacement for DPTM (neither was/is ISO/IEC 27001), nor is it a guarantee/protection against investigation or fines
  - Certificates contribute towards accountability, but they do not imply fulfilling the Accountability Obligation under the PDPA
  - In the context of DC and DI, it is the responsibility of the DC to assess the adequacy of such a certification by its DI, especially in terms of the Transfer Obligation (ISO/IEC 27701 certificate is also not a substitute/guarantee for CBPR, whereas DPTM is said to have incorporated CBPR specific elements)

Recent threat (vulnerability) landscape

Application Security Risks
2017 Top 10
A1-Injection
A2-Broken Authentication
A3-Sensitive Data Exposure
A4-XML External Entities (XXE)
A5-Broken Access Control
A6-Security Misconfiguration
A7-Cross-Site Scripting (XSS)
A8-Insecure Deserialization
A9-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring

Comparison of 2003, 2004, 2007, 2010 and 2013 Releases

OWASP Top Ten Entries (Unordered)	Releases				
	2003	2004	2007	2010	2013
Unvalidated Input	A1	A1[M]	X	X	X
Buffer Overflows	A5	A5	X	X	X
Denial of Service	X	A9[D]	X	X	X
Injection	A6	A6[D]	A2	A1[D]	A1
Cross Site Scripting (XSS)	A4	A4	A1	A2	A3
Broken Authentication and Session Management	A3	A3	A7	A3	A2
Insecure Direct Object Reference	X	A2	A4[D]	A4	A4
Cross Site Request Forgery (CSRF)	X	X	A5	A5	A8
Security Misconfiguration	A10	A10[D]	X	A6	A5
Missing Functional Level Access Control	A9	A2[D]	A10[D]	A8	A7[D]
Unvalidated Redirects and Forwards	X	X	X	A10	A10
Information Leakage and Improper Error Handling	A7	A7[D]	A6	A6[M]	X
Malicious File Execution	X	X	A3	A9[D]	X
Sensitive Data Exposure	A8	A8[D]	A8	A7	A6[M]
Insecure Communications	X	A10	A9[D]	A9	X
Remote Administration Flaws	A5	X	X	X	X
Using Known Vulnerable Components	X	X	X	X	A9[D][M]

Failure to understand shared responsibility of security in the cloud

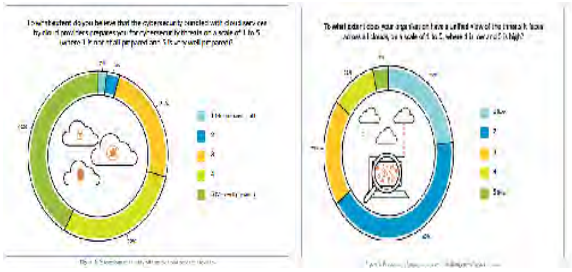


Figure 4 shows perceptions of security decision makers towards security bundled with cloud services. The research reveals that 70% of organisations view the security offered by cloud service providers for their discrete services to be sufficient. Indeed, the same proportion (70%) depends entirely on cybersecurity services provided by cloud providers for overall protection.

Source: https://www.paloaltonetworks.com/resources/apac-cloud-security-study Oct 2019

There are also various cloud deployment models…
the type and amount of control relinquished by the organisation vary. It is generally regarded that organisations have the least controls with public clouds.
The design and operations of cloud computing differ to some extent from non-cloud systems. Organisations that adopt cloud services for the management of personal data need to be aware of the security and compliance challenges that are unique to cloud services

Source: PDPC - GUIDE TO SECURING PERSONAL DATA IN ELECTRONIC MEDIUM

And as the pace of those changes to cloud computing platforms quickens, knowing exactly what settings can get you into trouble becomes exponentially more difficult to discern.

…all that flexibility…can come back to bite you later.. Misconfiguration drives the majority of incidents

Source: Sophos 2020 Threat Report

DREW & NAPIER

Ransomware

- **Data Encryption**: It encrypts personal files and folders (documents, spread sheets, pictures, and videos).
- **Lock Screen — WinLocker**: It locks the computer's screen and demands payment. It presents a full screen image that blocks all other windows. No personal files are encrypted.
- **Master Boot Record (MBR):** The Master Boot Record (MBR) is the part of the computer's hard drive that allows the operating system to boot up. MBR ransomware changes the computer's MBR so that the normal boot process is interrupted.
- **Encrypting web servers**: It targets webservers and encrypts a number of the files on it. Known vulnerabilities in the Content Management Systems are often used to deploy ransomware on web services
- **Mobile device**: Mobile devices (mostly Android) can be infected via "drive-by downloads". They can also get infected through fake apps that masquerade as popular services such as Adobe Flash or an anti-virus product.

Source: https://www.nomoreransom.org/

- 2017 was the raise of ransomware – 2018 showed raise in cryptojacking
- Ransomware still spreading but getting more customised towards high-value
- Cyber threat actors taking advantage of COVID 19 to conduct email scams, phishing and ransomware attacks.
- Ransomware attackers raise the stakes
- historically targeted personal and credit card information are increasingly turning to ransomware
- Crypto Miners, Targeted ransomware and cloud attacks dominate the threat landscape

Sources GovTECH, CSA, and MAS alerts Feb 2020, Sophos Threat Report/ CheckPoint/Fireeye research 2020

DREW & NAPIER

22

More sophistication for 2020 and beyond?

- For 2020, we predict advancements to be made in terms of how malware is delivered to PCs, including: more **sophisticated methods of spreading** threats via malicious emails; through a resurgence of exploit kits; via supply chain attacks; and by abusing the **Remote Desktop Protocol (RDP**).
- On the mobile side, we predict that more **subscription scams and fake apps** will make their way onto official app stores, and that more iOS vulnerabilities will be exposed by researchers and bad actors alike.
- In terms of Internet of Things devices, we predict devices and even physical locations will become smart or even smarter than they already are. We have already started to see cybercriminals taking steps to **further develop IoT malware**, including adding obfuscation to make it more difficult for analysts to analyze, and building upon exploit kits for smart devices.

Source: AVAST 2020 prediction
https://cdn2.hubspot.net/hubfs/486579/web-documents/2020_cybersecurity_predictions.pdf

Smart homes under siege
Threats on the move
Worms make a comeback

Social engineering online and by phone
All online accounts are fair game

Source: https://blog.trendmicro.com/the-everyday-cyber-threat-landscape-trends-from-2019-to-2020/

DREW & NAPIER

23

DREW & NAPIER