ISACA®

Trust in, and value from, information systems

2018 Top 10 Cyber Threats

@RaefMeeuwisse, ISACA Expert Speaker & author, ***Cybersecurity for Beginners***

Publications:

For ISACA

- GEIT for Health Care
- COBIT5 for Information Security (Update Only – not yet released)
- ISACA Now Blog

Independent Books

- Cybersecurity for Beginners
- The Cybersecurity to English Dictionary
- Cybersecurity: Home and Small Business
- Cybersecurity Exposed: The Cyber House Rules
- How to Keep Your Stuff Safe Online (Personal Cybersecurity)
- The Encrypted Pocketbook of Passwords

As a commentator

- Infosec Magazine
- Computer Weekly
- Sky News
- ZDNet
- TEISS News
- …

ISACA®
Trust in, and value from, information systems

The Cyber Risk Methodology Used

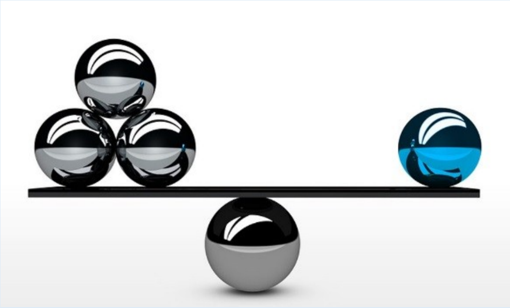
1

Reviewed articles & empirical data on cyber incidents & breaches, for example:

- Verizon Breach Incident Report 2017
- Juniper Research Cybercrime & The Internet of Threats 2017
- Ponemon Institute and Accenture Cost of CyberCrime Study 2017
- Ponemon Institute and IBM Cost of a Data Breach 2017
- Gartner Security Blog

2

Reviewed and analysed available advice and countermeasures



3

Applied risk scores to each risk

Probability	Impact
5. Very High	5. Very High
4. High	4. High
3. Medium	3. Medium
2. Low	2. Low
1. Very Low	1. Very Low

4

Generated a ***before*** and ***after*** risk score based o [redacted] security countermeasures

Cyber Threat Trends (Breach Statistics)

WHO?

- 75% due to external actors
- 25% involved internal actors (an attack by a malicious insider takes, on average, 50 days to resolve)
- 51% involved organized crime
- 18% conducted by state-affiliates
- 3% from multiple parties
- 2% from a partner

How Much?

- US$3.62m is the average total cost of data breach
- US$2.4m and US$2m costs for Malware and Web-based attacks respectively – making them the most costly attack types.
- US$2.8m cost savings on average when a company deploys security intelligence systems

WHY?

- 73% financially motivated
- 21% cyber espionage
- 1% grudge

HOW?

- 81% inc. stolen or weak passwords
- 62% involved hacking
- 51% involved malware (Malware attacks cost companies an average of US$2.4m annually)
- 66% of malware via email attachments
- 43% included a social angle
- 14% due to errors
- 14% due to privilege account misuse
- 27.7% is the likelihood of a recurring material data breach over the next two years

Selected breach metrics from:

- Verizon 2017 DBIR,
- Ponemon/IBM 2017 Cost of a Data Breach Report 2017
- Accenture/Ponemon Cost of Cyber crime Study 2017

The Biggest Cyber News Stories of 2018...

Malware

- Cryptojacking
- Fileless Malware

DDoS

- Largest DDoS Attack ever
- Followed by an even larger one

Data Misuse

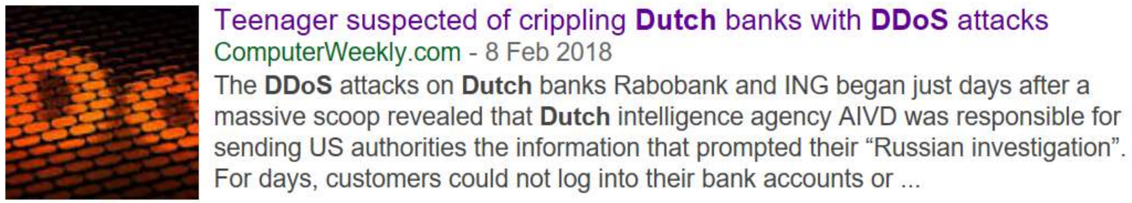
- Cambridge Analytica
- “Senator. We sell ads.”

0 day (zero day)

- Meltdown & Spectre
- Slingshot
- ...

In the Netherlands

- ...



Teenager suspected of crippling **Dutch** banks with **DDoS** attacks
ComputerWeekly.com - 8 Feb 2018
The **DDoS** attacks on **Dutch** banks Rabobank and ING began just days after a massive scoop revealed that **Dutch** intelligence agency AIVD was responsible for sending US authorities the information that prompted their “Russian investigation”. For days, customers could not log into their bank accounts or ...

The 2018 Cyber Risk Top 10*

Based on **residual risk** scores in environments where the latest available security measures are implemented.

- *No guarantee is made on these risk scores – as they are based on individual analysis and may not reflect the opinion of ISACA*
- *The level of risk in each environment is always unique and differs from organization to organization.*

ISACA
Trust in, and value from, information systems

IoT and Smart Appliances (excluding DDoS)

Risk Description

Interconnected devices in homes and offices - potentially build on unsecured firmware, open ports by default, and difficult to patch

	Probability	Impact	Risk Score
Unadjusted Risk	4. High	5. Very High	20

Example Countermeasures

Securing all connections if possible, network analytics and traffic monitoring to find unusual traffic, patch where possible, stringent matching identity and access practices. Treat SMART devices as inherently non-secure & risky.

	Probability	Impact	Risk Score
Adjusted Risk	3. Medium	3. Medium	9

CISCO estimates that 40 billion devices will be connected to the Internet by 2020 as cars, fridges, medical devices and gadgets not yet imagined or invented will link in, which will lead to the tremendous growth of threats and vulnerabilities in 2018 through 2020.

Unreliable External Technology (Eg. Cloud Outages)

10

Risk Description

Major outages are more regular for substantial online tech platforms, including the large cloud providers where critical operational dependencies may exist.

	Probability	Impact	Risk Score
Unadjusted Risk	4. High	5. Very High	20

Example Countermeasures

Contingency planning, failover architecture, alternative suppliers, retaining business critical activities in guaranteed / insured high reliability environments...

Adjusted Risk	3. Medium	4. High	12

Can also be a critical dependence on a supplier (non-technology) that has a failure in their technology, or experiences a substantial cyber attack.

(6) ↓ 9

Existing vulnerabilities

Risk Description

Vulnerabilities that are already known to security teams, as well as attackers, and which are not yet protected against

	Probability	Impact	Risk Score
Unadjusted Risk	5. Very High	5. Very High	25

Example Countermeasures

Patching where possible, perimeter and defences where device patch not possible, active vulnerability scans, APT monitoring and analytics

Adjusted Risk	5. Very High	3. Medium	15

SANS estimates that over 80 percent of cyber security incidents exploit known vulnerabilities, and the annual Verizon Data Breach Investigation report shows similar numbers. Gartner comes in much higher, estimating that “through 2020, 99 percent of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

Trust in, and value from, information systems

DDoS including IoT DDoS

➔ 8

Risk Description

Using botnets and hijacked devices to bombard a location with an overwhelming number of data requests sufficient to prevent normal operation. Can potentially be a mask for another malicious activity

	Probability	Impact	Risk Score
Unadjusted Risk	5. Very High	5. Very High	25

Example Countermeasures

DDoS filtering services, alternative failover service locations, edge services …

	Probability	Impact	Risk Score
Adjusted Risk	5. Very High	3. Medium	15

The size and scale of DDoS attacks have increased and the cost to attackers has lowered. Small attacks can be filtered but attack sizes of size can disrupt.

Digital transformation

(5) ↓ 7

	Probability	Impact	Risk Score
Risk Description	Organisational change associated with/driven by the application of digital technology		
Unadjusted Risk	4. High	5. Very High	20
Example Countermeasures	Full risk assessments of all new technologies, cultural change programmes to enure buy-in, investment in appropriate rather than revolutionary technologies		
Adjusted Risk	3. Medium	5. Very High	15

Those organizations that are slow to invest in and implement digital transformation will find themselves at an increasingly pronounced competitive disadvantage in their respective industries.

ISACA®
Trust in, and value from, information systems

Malware including Ransomware, Fileless, Cryptojacking

(4) ↓ 6

Risk Description

Malicious software, including metamorphic and polymorphic varieties, designed to spread, steal, corrupt, control or ransom system contents

	Probability	Impact	Risk Score
Unadjusted Risk	5. Very High	5. Very High	25
Adjusted Risk	5. Very High	3. Medium	15

Example Countermeasures

Rapid patch management, effective AI anti-malware, restricted installation permissions, robust backup and recovery procedures...

In the US Office of Personnel Management (OPM), an AI anti-malware was installed after the breach and found over 2000 previously undiscovered malware threats.

Web Application Attacks

(3) ↓ 5

Risk Description

The targeting of software that operates over networks using OWASP type vulnerabilities such as cross-site scripting, SQL injection or other vulnerabilities.

	Probability	Impact	Risk Score
Unadjusted Risk	5. Very High	5. Very High	25
Adjusted Risk	5. Very High	3. Medium	15

Example Countermeasures

Use a secure development lifecycle, security requirements by design, static source code testing, pen testing before release, ongoing monitoring, IDPS, ...

Any major online or web services are a major target for attack and require continuous efforts to remain adequately secure.

NEW ENTRY 4

Zero Day (including ‘outed’ Nation State Tools)

	Probability	Impact	Risk Score
Risk Description	The emergence of a previously unknown exploit for which at point of discovery, there is no commercial patch yet available. Eternal Blue, Slingshot, Spectre, Meltdown were all zero day threats when first publicised.		
Unadjusted Risk	4. High	5. Very High	20
Example Countermeasures	Active threat intelligence, robust defence-in-depth, AI security technologies such as AI anti-malware, ...		
Adjusted Risk	4. High	4. High	16

GDPR-General Data Protection Regulation, an EU regulation, will become applicable to every country in the world in May 2018.

Trust in, and value from, information systems

Data Theft

(7) ↑ 3

Risk Description

The theft of credentials, intellectual property, customer details and other items that may be of high resale value. GDPR ransom value and the brand devastation of data theft has increased the target value, especially for PI.

Unadjusted Risk

Probability	Impact	Risk Score
5. Very High	5. Very High	25

Example Countermeasures

Having an accurate information asset register, data loss prevention software, application level security controls, audit trails, privileged account management, ...

Adjusted Risk

Probability	Impact	Risk Score
4. High	5. Very High	20

Often data thefts can emerge years after the initial incident took place (e.g. Yahoo). Most likely to create substantial brand and company value damage if successful.

2

Phishing & Smart Phishing

Risk Description

Creating electronic communications that pretend to come from a legitimate source to acquire sensitive information or install malware.

	Probability	Impact	Risk Score
Unadjusted Risk	5. Very High	5. Very High	25

Example Countermeasures

Containerization, AI anti-malware, patch operating systems, remove admin privileges, URL filtering, staff education, email filters, phishing simulations. PROBLEM – Authorised people are still vulnerable despite tech defences.

Adjusted Risk	5. Very High	4. High	20

According to Symantec, one in 131 emails contained malware, the highest rate in five years.

ISACA®
Trust in, and value from, information systems

Privacy (including GDPR)

➡ 1

Risk Description	Regulations such as GDPR, ePrivacy and others come with onerous data governance requirements, and serious repercussions for failure to comply		
	Probability	Impact	Risk Score
Unadjusted Risk	5. Very High	5. Very High	25
Example Countermeasures	Programme of data discovery, asset management and process governance as well as orchestrated identity management and coordinated compliance efforts with privacy and business functions. Clear roles and responsibilities.		
Adjusted Risk	4. High	5. Very High	20

GDPR-General Data Protection Regulation, an EU regulation, will become applicable to every country in the world in May 2018.

ISACA®
Trust in, and value from, information systems

But What Happens Without Executive Support?

	Residual Risk [Secure Environments]
1	[20] Global Regulations (including GDPR)
2	[20] Phishing & Smart Phishing
3	[20] Data Theft
4	[16] Zero Day
5	[15] Web Application Attacks
6	[15] Malware inc. Fileless & Cryptojacking
7	[15] Digital Transformation
8	[15] DDoS including IoT DDoS
9	[15] Existing Vulnerabilities
10	[12] Unreliable External Technology

		Inherent Risk [Non-Secure Environments]
	1	[25] Global Regulations (including GDPR)
	2	[25] Phishing & Smart Phishing
↑	3	[25] Data Theft
↑	4	[25] Web Application Attacks
↑	5	[25] Malware inc. Fileless & Cryptojacking
↑	6	[25] DDoS including IoT DDoS
↑	7	[25] Existing Vulnerabilities
New Entry	8	[25] Human Error
↓	9	[20] Zero Day threats
↓	10	[20] Digital Transformation

Best Practices to Reduce Cyber Risk

- Have an empowered and accountable CISO on the main board
- Never allow the use of unsupported or unpatched devices for data of value
- Install effective AI based anti-malware (check efficacy and stay up to date)
- Containerize wherever practical – avoid networking devices
- Time to upgrade anything of value from single factor password authentication

But mainly

- Convince your executive to invest in the right security at the right time
- Stay up to date on the latest threats and effective defences
- Remember that considering the security budget in a silo is a false economy