Cybersecurity

Dr. Uwe Glässer - Instructor
Professor, Computing Science
email: cybersec@sfu.ca

Seyed Amir Yaghoubi Shahir - TA
PhD student, Computing Science
email: sayaghou@sfu.ca

Perspective

- This course introduces cybersecurity concepts and discusses cyber intelligence and threat analysis methods in the context of Big Data analytics.
- Cyber situational analysis and anomaly detection based on probabilistic modelling will play a central role.
- This includes using the R language and software environment for statistical computing.
- Fundamental concepts and applied aspects of cybersecurity risk assessment and management will be discussed in detail.
- Prerequisites CMPT 225. Additional prerequisites to be determined …

  STAT 270, MATH 232 (or MATH 240) — not mandatory.

Practicalities

- Office Hours

  Wednesdays, 4:00-5:00 PM, TASC 1 - Rm 9239 (my faculty office)

  Mondays, 4:00-5:00 PM, Rm: CSIL - TBA (Amir)

  Office hours may end after 30 minutes in case of no attendance.

- Special Session

  Prior to the last week of classes, Nov 26-30: 1-2 extra hours may be needed for course project presentations - date/time/room: TBA (Wed Nov 28, 12:30-2:00?)

  Last week of classes: **project final test** - during regular class hour

- Tutorials

  R language and software environment for statistical computing

  During regular class hours as announced

- Final Exam

- Course Materials

  Slides will be posted regularly right after class

  Reading materials will be posted as needed

  No textbook covering the entire curriculum

- Course Page

  https://coursys.sfu.ca/2018fa-cmpt-318-d1/

- Midterm, Tests

  Midterm exam will be held **October 22-26 (tentatively)**

  Tests will be announced one week ahead.

  Short questions with concise answers

- Assignments

  Reading assignments

  Marked assignments

- Class participation

  Accounts for up to 5% of the final grade

- Course Project

  Group project with teams of 4-5 team members

  Documentation of **who contributed what** to the project

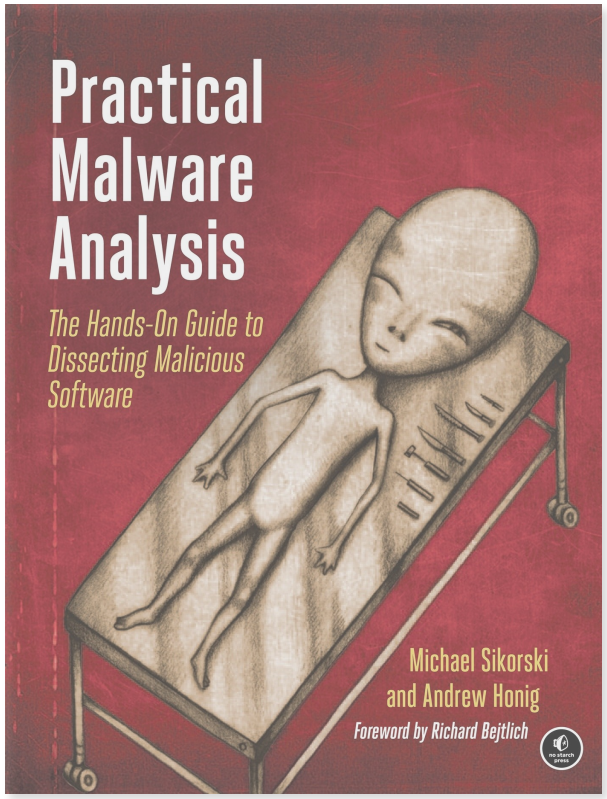
  Meet early and meet often to overcome logistic challenges.

  Project is organized in three separate parts

  Project groups will be finalized **end of next week** - notify Amir regarding your preferences!

- Course Scope

  What this course is **not** about …



"With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way."

Learning outcomes …

- Cybersecurity Curricula 2017

  Joint Task Force on Cybersecurity Education

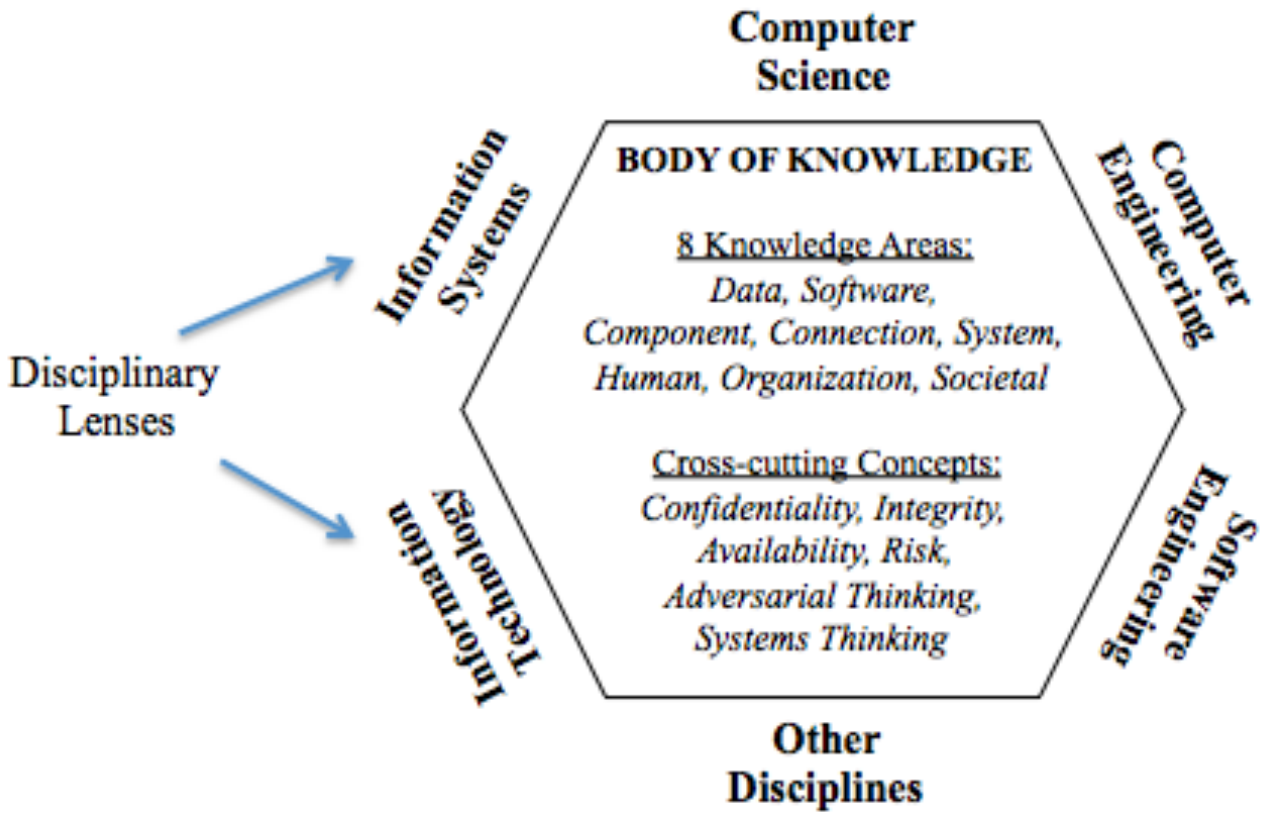
  - Association for Computing Machinery (ACM)
  - IEEE Computer Society (IEEE-CS)
  - Association for Information Systems (AIS)
  - International Federation for Information Processing (IFIP)

  Version 1.0 Report - 31 December 2017 defines '***The Cybersecurity Discipline***' as:

  A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management.

  While cybersecurity is an interdisciplinary course of study including aspects of law, policy, human factors, ethics, and risk management, it is fundamentally a computing-based discipline.

  Crosscutting concepts help students explore connections among the knowledge areas, and are fundamental to an individual's ability to understand the knowledge area regardless of the disciplinary lens. These concepts provide *an organizational schema for interrelating knowledge* into a **coherent view of cybersecurity**.



Section 1

Cybersecurity - Introduction

Why do we care?

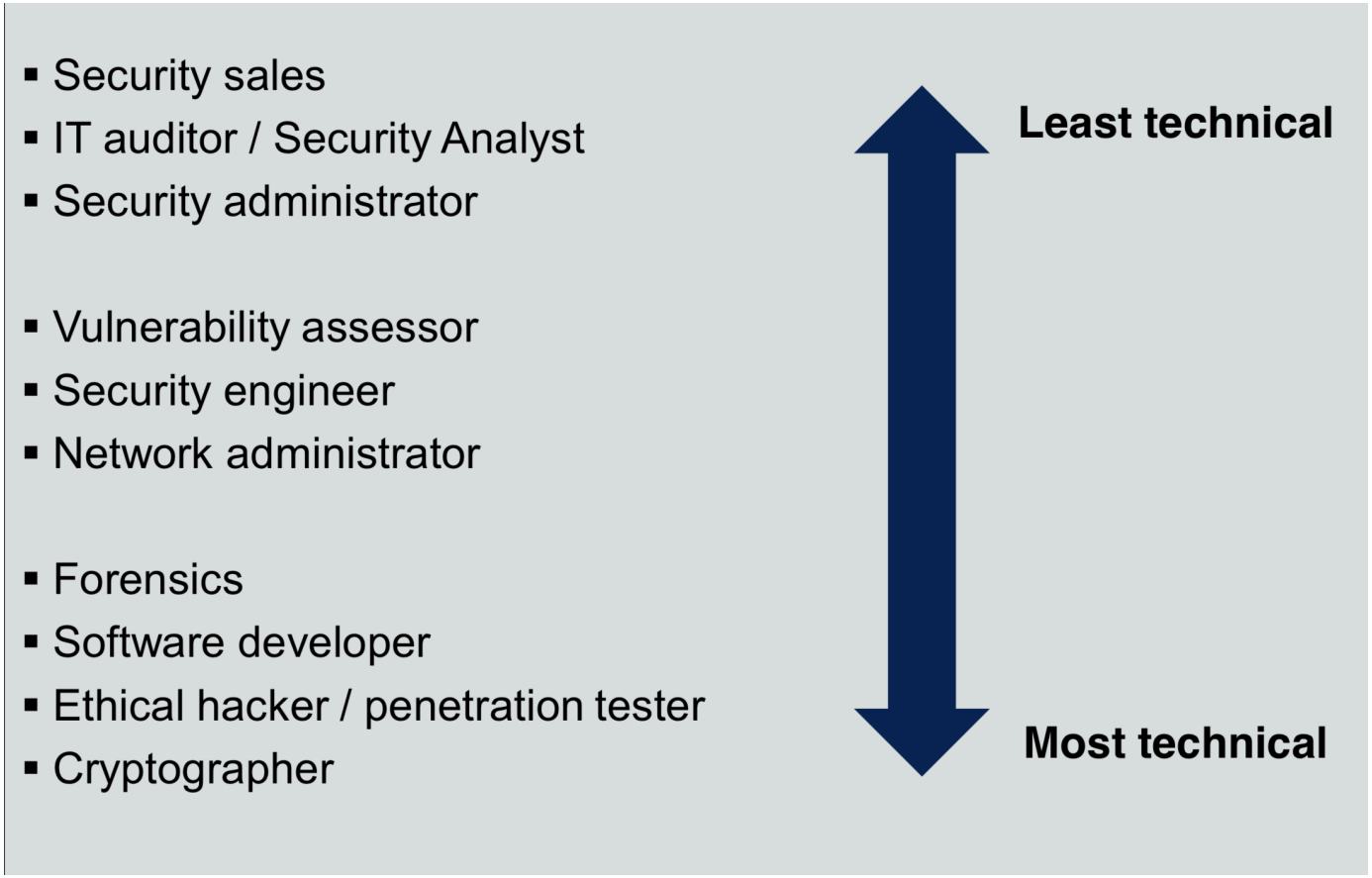
Discussion

1. What does it mean to YOU?
2. Are YOUR concerned personally?
3. Future impact on individuals, economy, society?

Source: CartoonStock

Career perspectives

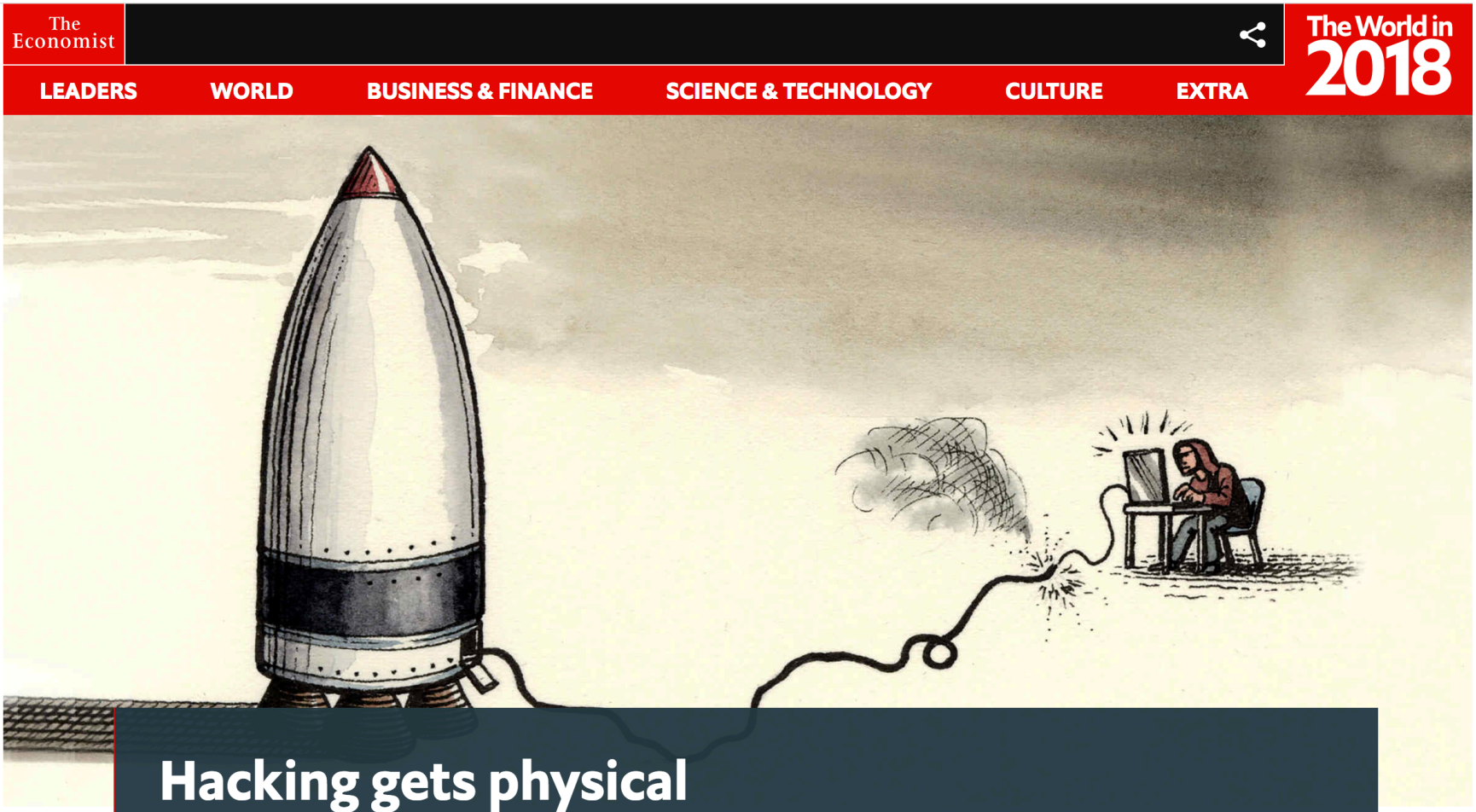
Source: ISACA, Vancouver



BC AWARE DAY, January 30, 2018
http://www.bcaware.ca/2018/

Evolving threat landscape

Cyberattacks are becoming increasingly routine, and are a complex and evolving threat. Information security breaches frequently compromise protection of sensitive data and information, exposing personal identities, intellectual property, or financial assets. This causes substantial damage that can ruin lives and businesses. Even more troublesome, such attacks go often unnoticed for extended periods of time. Still, things can get a lot worse when cyberattacks target distributed control systems essential for operating critical infrastructure such as water management systems, electric power grids, and intelligent transportation systems. Besides temporal disruption of critical services, sophisticated attacks may cause physical damage to vital system components, and ultimately even threaten human safety.



"Target, Yahoo, Equifax: the list of prominent victims of cyber-attacks is already long, and will surely lengthen further in 2018. But in the year ahead security types will also be worried about the next, potentially even scarier generation of hacking. It could cause physical, not just financial, harm.

In industrialised countries critical national infrastructure, including **hospitals, railways and even nuclear defence systems**, cannot be hacked only through its connection to a network. It also relies on a constant stream of data to operate efficiently. Weather stations, airports, motorways and power plants react to incoming information on a **minute-by-minute, even second-by-second**, basis. But what if such data could be faked by saboteurs? … There's incontrovertible evidence that spoofing occurred," says Todd Humphreys, of the University of Texas at Austin.

Mr Humphreys believes **transport networks** are particularly vulnerable. He also worries about the New York Stock Exchange. Traders use a signal from an atomic clock, operated by the National Physical Laboratory, which he says could be spoofed.

The **purpose of attacks** on critical infrastructure in the near future would probably be to undermine trust, embarrass enemies and test hacking capabilities, rather than cause physical harm."

Critical Infrastructure

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. … Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

Source: Public Safety Canada

Critical Infrastructure Sectors

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

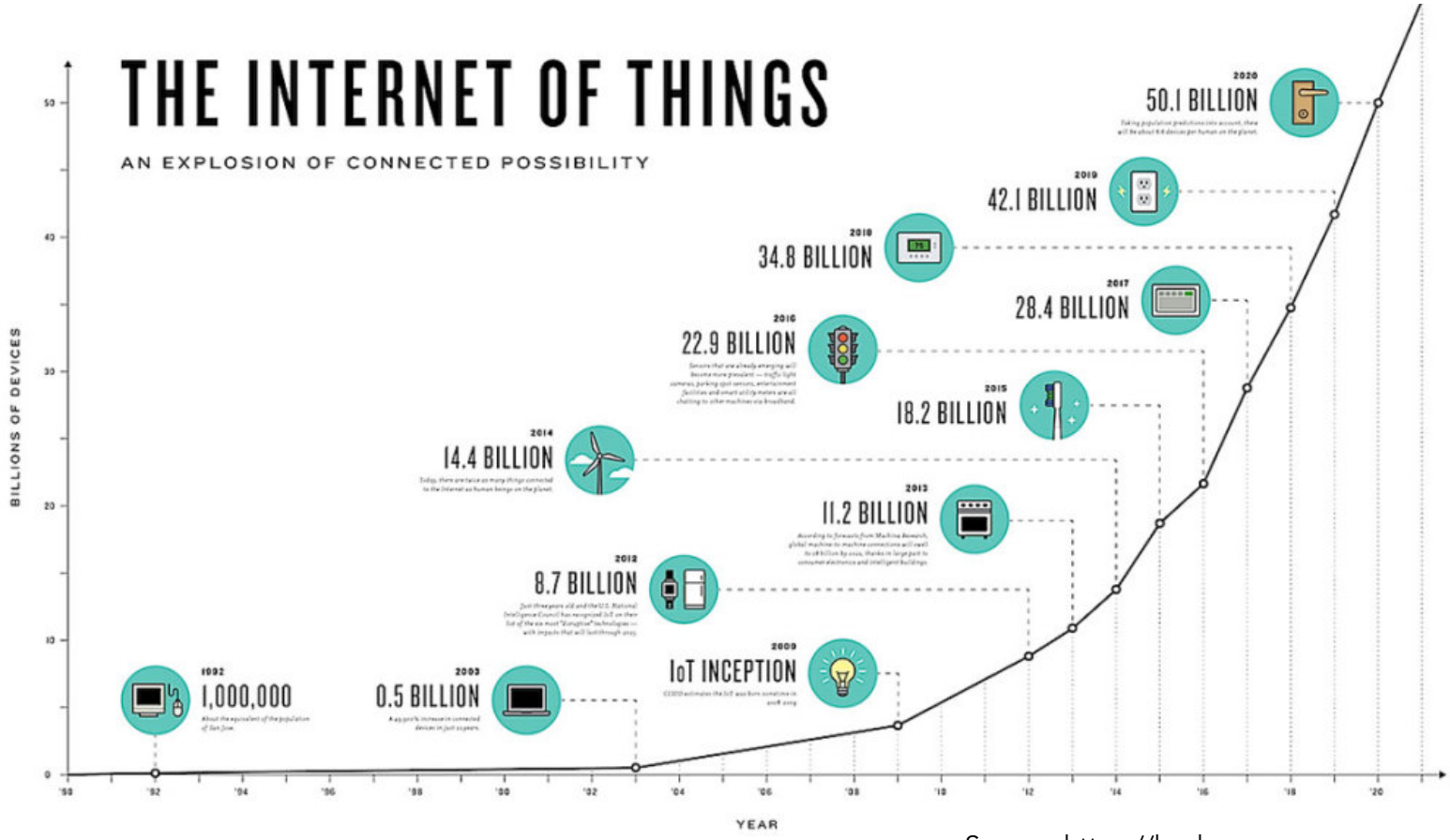
Source: US Homeland Security

https://www.dhs.gov/critical-infrastructure-sectors

Cybercrime

10 Dark Secrets of Cybercrime

https://www.youtube.com/watch?v=B044J01U7Qk



Source: https://hackernoon.com

Source: Wikipedia

Here goes your privacy …

A simple definition of cybersecurity

"To understand the term cybersecurity, we must first define the term cyberrisk.

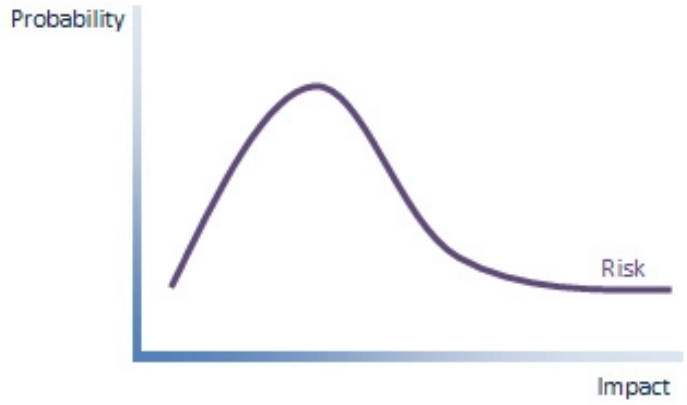


Figure 1

Cyberrisk is not one specific risk. It is a **group of risks**, which differ in technology, attack vectors, means, etc. We address these risks as a group largely due to two similar characteristics: A) they all have a potential great impact B) they were all once considered improbable.

To understand this we start with a visual representation of the traditional risk curve:

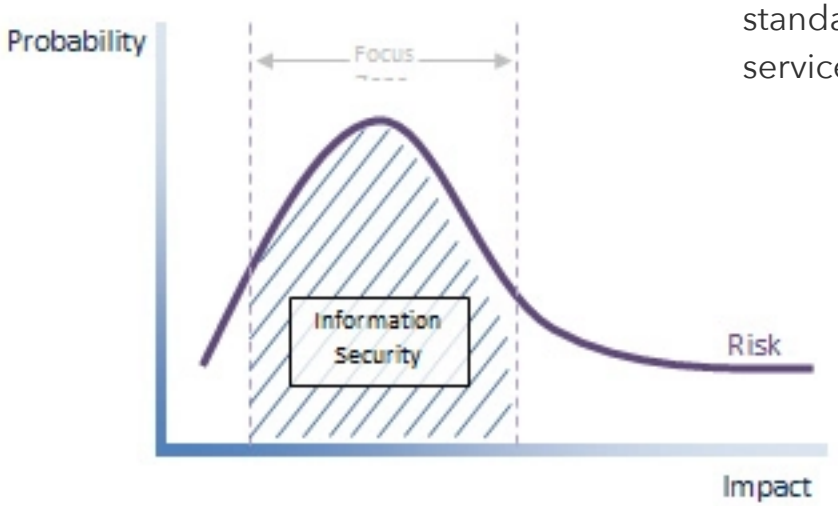
Figure 1 is a simple graph that shows the correlation between the probability of a risk occurrence and its potential impact. As we move to the right, risk's potential impact increases. At the far right of the risk curve we see a "long tail"—a group of very high impact risks with a very low probability of occurrence. (Naturally, organizations have resource constraints and focus their efforts on addressing the risks with high probability of occurrence and potentially significant impact.)"

Source: Barzilay, 2017

"Next, let us define **focus zone** (depicted in Figure 2 below) as the area containing the risks to which the organization directs its mitigation efforts. The size of the focus zone is determined by factors such as risk appetite, cost effectiveness, the CISO's attitude, organizational culture, availability of resources and relative threat landscape.

As illustrated below, the efforts invested in addressing risks within the focus zone are commonly referred to as information security. Those risks include traditional malwares (viruses, trojans, spyware, adware, etc.), standard phishing attacks, standard distributed denial of service (DDoS) attacks, standard hacking activities, etc."

Figure 2



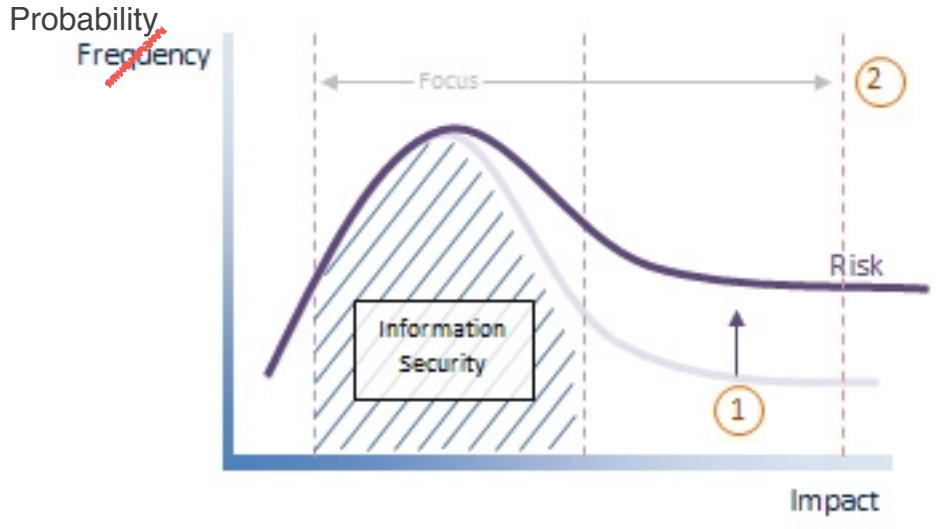
Source: ISACA News, 2017

"Of course, something has changed recently. The threat landscape evolved to the point that risks that were once considered unlikely began occurring with regularity. The increased probability of **very-high-impact risk occurrences** is illustrated in Figure 3 below as Item 1.

This trend can be attributed to higher maturity of attack tools and methods, increased exposure, increased motivation of attackers, and better detection tools enabling more visibility. With that said, we must accept that some of this shift is a result of our **increased awareness** to this new, highly focused group of risks.

The change to the threat landscape forces us to expand an organization's focus zone to include these previously excluded risks—illustrated below as Item 2."

Figure 3

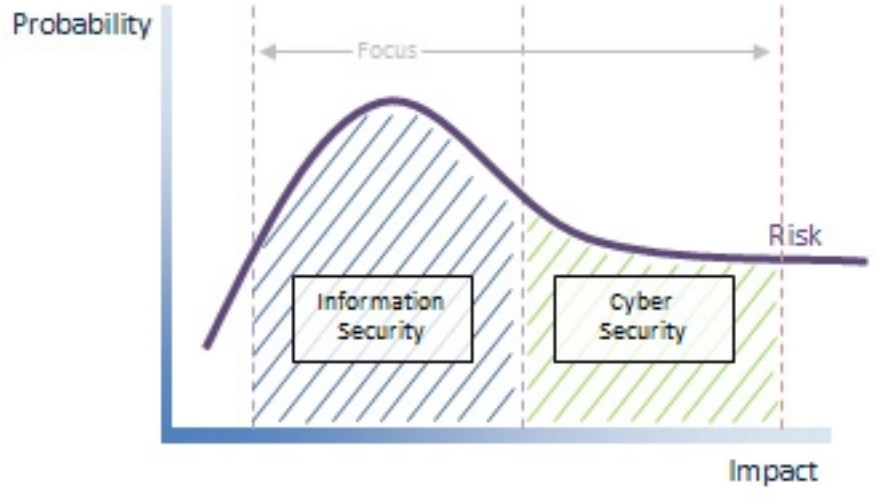


Source: ISACA News, 2017

"This new group of very-high-impact risks that now requires our attention is commonly referred to as cyberrisk. As illustrated in Figure 4 below, efforts invested in addressing cyberrisks are known, naturally, as cybersecurity.

This group of risks includes all sorts of strange scenarios: organization specific, specially designed malwares; manipulated hardware and firmware; the usage of stolen certifications; spies and informants; exploiting vulnerabilities in archaic hardware; attacking third party service providers; etc. This list also includes what are known as **advanced persistent threats**."

Figure 4



Source: ISACA News, 2017

"Some might consider information security and cybersecurity as two different disciplines, but I would argue that cybersecurity is a subdiscipline of information security (see Figure 5).

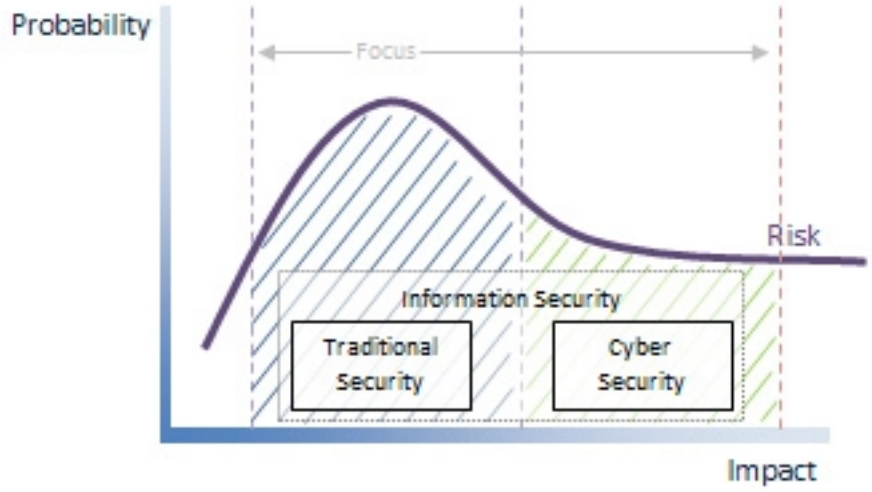


Figure 5

Cybersecurity is the sum of efforts invested in addressing cyberrisk, much of which was, until recently, considered so improbable that it hardly required our attention.

We must remember that the shift of the risk curve represents an ongoing trend. Very-high-impact risks will become increasingly frequent, forcing us to become better at protecting assets and devising creative solutions to mitigate risks."

Source: ISACA News, 2017

Advanced Persistent Threats

An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or group targeting a specific entity (either a private organization, a state or both for business or political motives).

APT processes require a high degree of covertness over a **long period of time**:

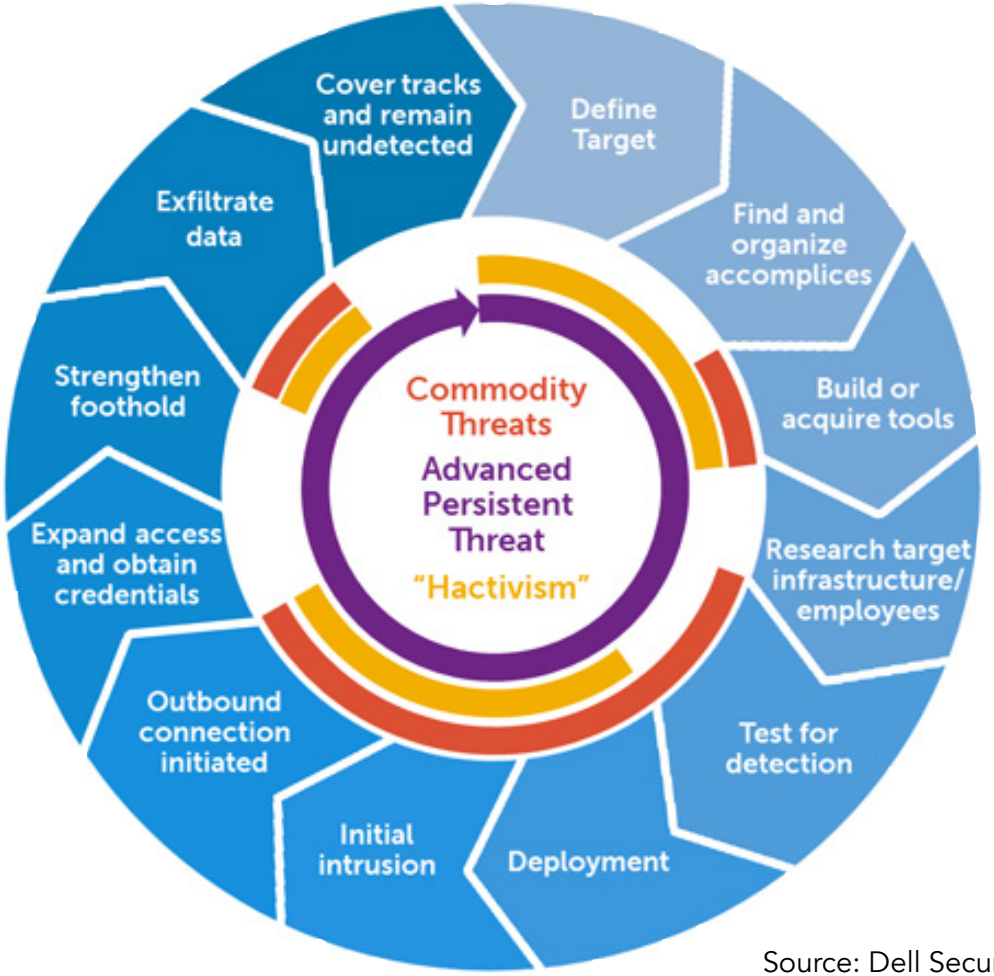
- *advanced* signifies sophisticated techniques using malware to exploit vulnerabilities in systems;
- *persistent* suggests that an external command and control system is continuously monitoring and extracting data from a specific target;
- *threat* indicates human involvement in orchestrating the attack.

APT usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity.

The term is commonly used to refer to cyber threats, in particular espionage using a variety of intelligence gathering techniques to access sensitive information. The purpose of these attacks is to place custom malicious code (through social engineering and spear phishing) on computers for specific tasks and to **remain undetected** for the longest possible period.

Kill chain

Actors behind advanced persistent threats create a growing and changing risk to organizations' financial assets, intellectual property, and reputation by following a continuous process, the kill chain.



Source: Dell SecureWorks

Commodity threat means casting the net wide, not knowing what specific targets may be compromised.

Hactivism is the subversive use of computers and computer networks to promote a political agenda or a

Target Data Breach

Source: Krebs on Security, a leading security news and investigation blog
http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Anatomy of the breach

What likely happened and how the company could have prevented the hack: Missed opportunities and lessons learned

In December of 2013, Target Corp. announced that **40 million customer debit and credit cards** were compromised. Shortly after the data breach, the retailer hired security experts at Verizon to probe its networks for weaknesses. Within one week, the security consultants reported that they were able to crack 472,308 of Target's 547,470 passwords (86 percent) that allowed access to various internal networks.

The attack started on November 27, 2013. Target personnel discovered the breach and notified the U.S. Justice Department by December 13th. The breach appears to have begun on or around **Black Friday 2013**—by far the busiest shopping day of the year.

Top 4 passwords:

Jan3009# - 4312 (0.91%)
sto$res1 - 3834 (0.81%)
train#5 - 3762 (0.8%)
t@rget7 - 2260 (0.48%)

Attack surface

Verizon's findings support the theory about how hackers initially broke into Target. Fazio Mechanical, a small HVAC contractor in Pennsylvania that worked with Target, had suffered a breach via malware delivered in an email. In that intrusion, the thieves managed to steal the **virtual private network credentials** that Fazio's technicians used to remotely connect to Target's network.

"Once inside Target's network, there was nothing to stop attackers from gaining **direct and complete access** to every single cash register in every Target store." Altogether, the attackers stole 11 GB of data.

Target's password policies in effect at the time may have been based on **password management best practices**, but it appears most internal standards were never followed. "While Target has a password policy, the Verizon security consultants discovered that it was not being followed. The Verizon consultants discovered a file containing valid network credentials being stored on several servers. They also discovered systems and services utilizing either weak or default passwords. Utilizing these weak passwords the consultants were able to instantly gain access to the affected systems …" including target.com, corp.target.com; email.target.com; stores.target.com; hq.target.com; labs.target.com; and olk.target.com.

"The Verizon assessment, conducted between December 21, 2013 to March 1, 2014, notably found **no controls limiting their access to any system**, including devices within stores such as point of sale (POS) registers and servers. Consultants were able to directly communicate with point-of-sale registers and servers from the core network. In one instance, they were able to communicate directly with cash registers in checkout lanes after **compromising a deli meat scale** located in a different store.

Verizon's report offers a likely playbook for how the Target hackers used that initial foothold provided by Fazio's hack to push malicious software down to all of the cash registers at more than 1,800 stores nationwide."

Cyber Fusion Center

"Target has never talked publicly about **lessons learned** from the breach, no doubt because the company fears whatever it says will be used against it in class-action lawsuits. However, the company has invested hundreds of millions of dollars in additional security personnel and in building out a "cyber fusion center" to better respond to daily threats that confront its various stores and networks."

Target's "Cyber Fusion Center." Image: target.com

Threat, Vulnerability, and Risk

These three security terms are often mixed up or used incorrectly. Clearly differentiate their meaning to avoid confusion. Using these terms interchangeably defeats the purpose.

Note: "Risk assessment" and "threat assessment" are entirely different things.

Asset

People, property, and information.

- Employees and customers along with other invited persons such as contractors or guests.
- Tangible and intangible assets that can be **assigned a value**. Intangible assets include intellectual property, reputation and proprietary information such as trade secrets.
- Databases, software code, critical company records, and many other intangible items.

An asset is what we are trying to protect.

Threat

Anything that can exploit a vulnerability

- intentionally or accidentally, and
- obtain, damage, or destroy an asset.

A threat is what we're trying to protect against.

Vulnerability

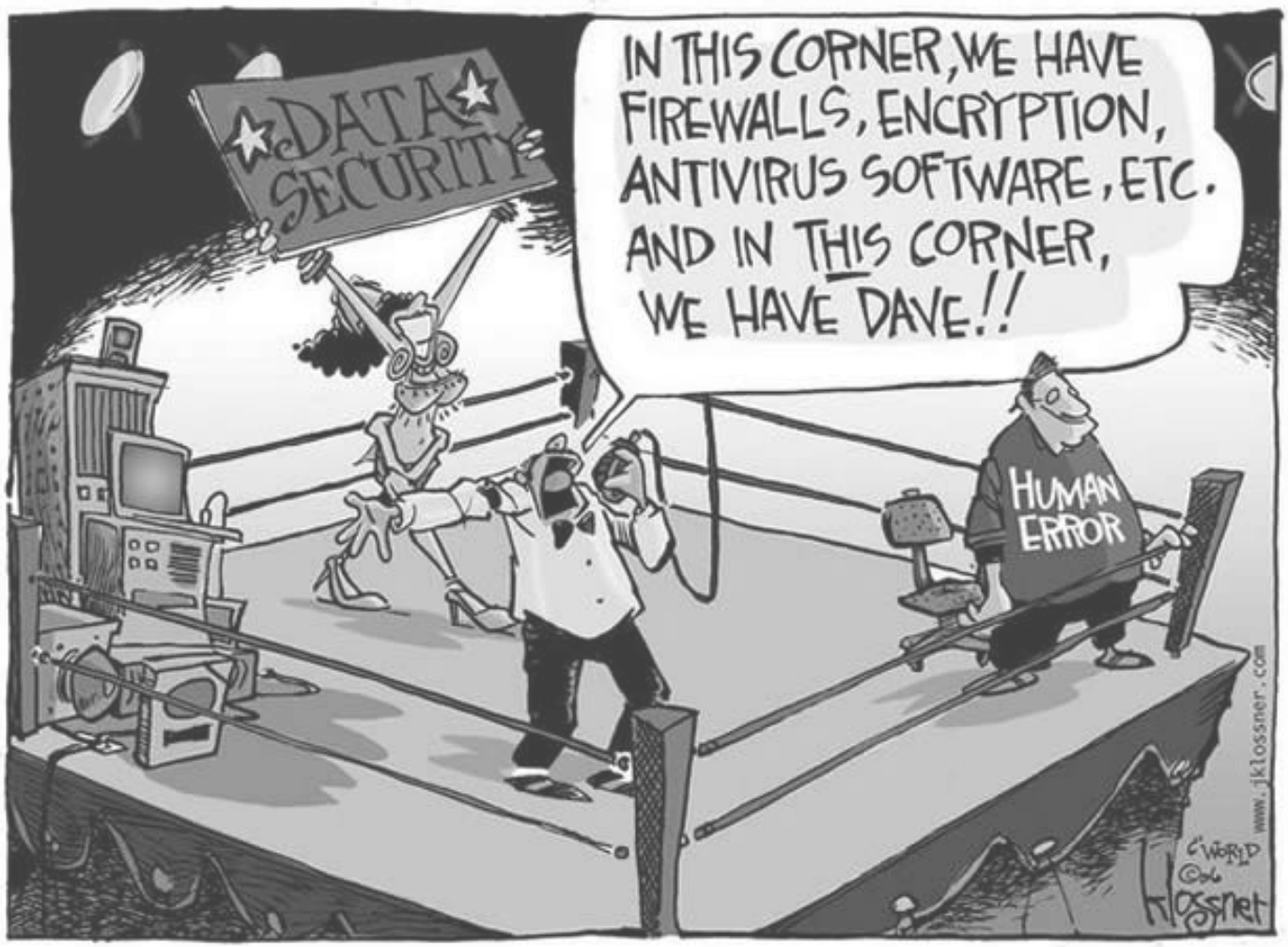
Weaknesses or gaps in a security program
that can be exploited by threats to gain unauthorized access to an asset.

A vulnerability is a weakness or gap in our protection efforts.

The term vulnerability refers to security flaws in a system that allow an attack to be successful.

Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed. Vulnerabilities are not limited to technology – they can also apply to social factors such as individual authentication and authorization policies.

Example: a penetration test, colloquially known as a pen test, is an authorized simulated attack on a computer system, performed to evaluate the security of the system.



Risk

The potential for loss, damage or destruction of an asset
as a result of a threat exploiting a vulnerability.

Risk is the intersection of assets, threats, and vulnerabilities.

Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to assets. Differentiating between threats, vulnerabilities and risk is the first step.

Source: Threat Analysis Group, LLC
https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

Risk Assessment

When conducting a risk assessment, the formula used to determine risk is

$$\text{Risk} = \left(\frac{\text{Vulnerability } x \text{ Threat}}{\text{Counter Measure Score}}\right) x \text{ Valuation}$$

Risk is **a function of threats exploiting vulnerabilities**.

The valuation is the estimated value to the organization of the asset that is at risk.

Countermeasures are specific actions we put in place to mitigate threats, for example we might put in place a firewall to stop unauthorized access to servers and data within our environment.

Risk calculation is a significant part of a business case, as it will allow you to calculate the Return of Investment (ROI) you are likely to achieve by implementing a new countermeasure.

A common approach to risk estimation ..

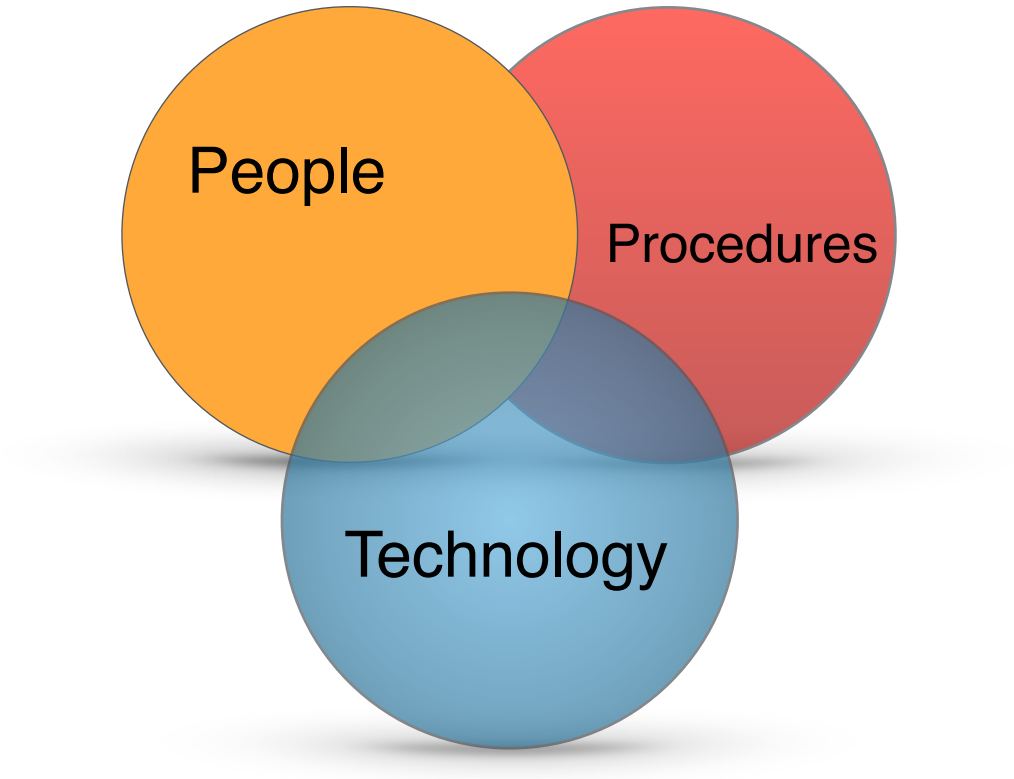
RISK

CONSEQUENCE			
EXTREME	HIGH	HIGH	EXTREME
HIGH	MEDIUM	HIGH	EXTREME
MEDIUM	MEDIUM	MEDIUM	HIGH
LOW	LOW	MEDIUM	HIGH
	UNLIKELY	POSSIBLE	LIKELY

THREAT + VULNERABILITY

.. that may do more harm than good.

Cybersecurity Strategy



A comprehensive view of cybersecurity is critical.

The Defender's Dilemma

"Cybersecurity is a constant and, by all accounts, growing challenge. Although software products are gradually becoming more secure and novel approaches to cybersecurity are being developed, hackers are becoming more adept and better equipped. Their markets are flourishing and the value at stake is growing. The rising tide of network intrusions has focused organizations' attention on how to protect themselves better. But some are now asking how much longer today's approach to cybersecurity will remain viable before something radically new will be needed."

Source: RAND Corporation, Martin C. Libicki et al. 2015

NOTE: RAND National Security Research Division (NSRD) conducts research and analysis on defence and national security topics for the U.S. and allied defence, foreign policy, homeland security, and intelligence communities and … nongovernmental organizations that support defence and national security analysis.

The Measure-Countermeasure Dance between Defender and Attacker

Measures and countermeasures to mitigate the likelihood of an attack

Attackers just have to be lucky once, but defenders have to look at all potential risks.

⚐ Objective: managing cyber risks to an **acceptable level**

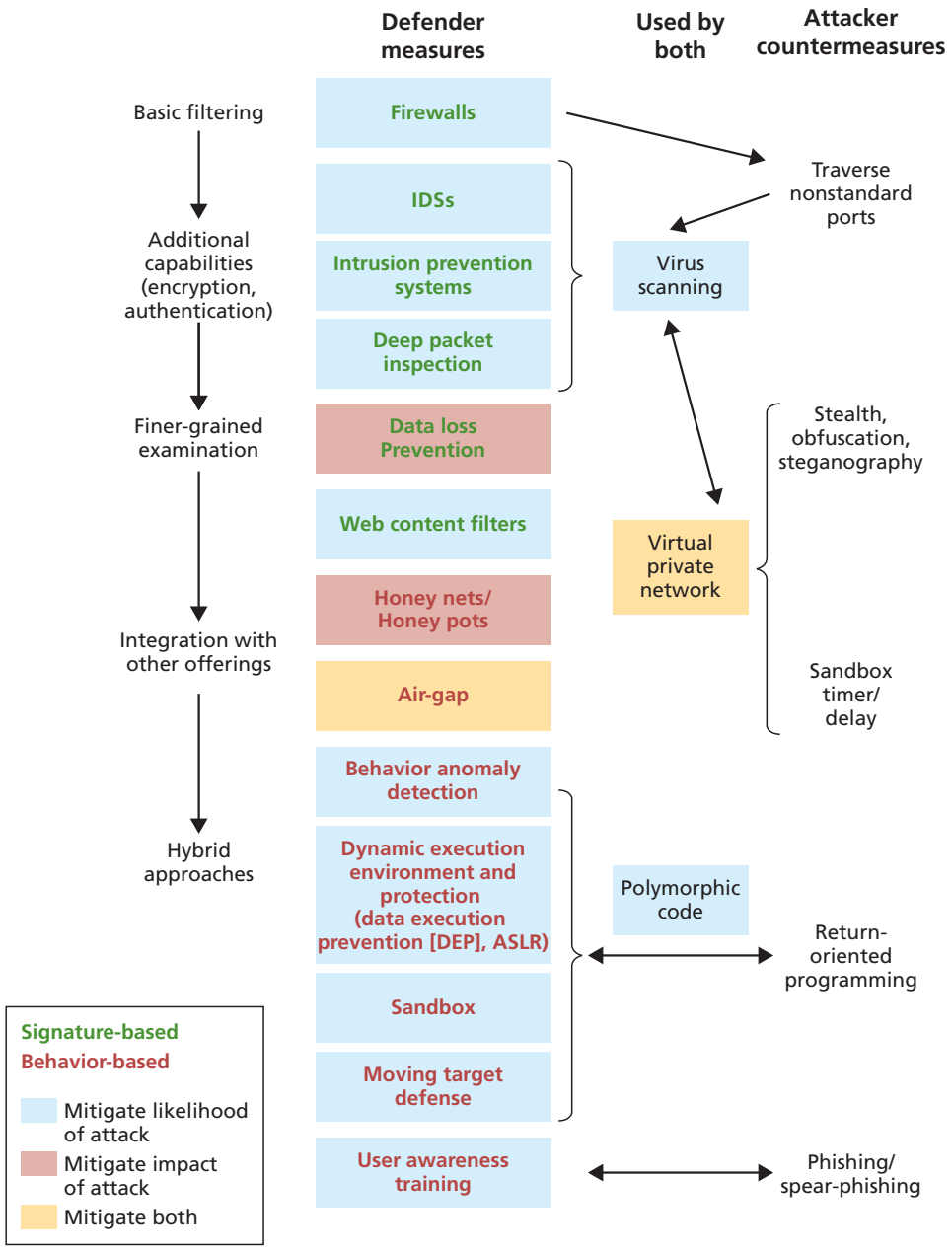
Firewalls, Intrusion Detection Systems (IDS), …

a device or software application that monitors a network or systems for malicious activity or policy violations.

*"All these approaches have to do with defenders improving the fidelity with which they identify the presence of attacker code on their systems. But there are also a class of defensive approaches that assume **attackers will get through no matter what** is done to stop them, reasoning that it is fundamentally impossible to get an encyclopedic list of malware signatures. These approaches focus on mitigating the impact of attacks and rely on such methods as deceiving attackers about the identity of information resources or isolating the execution of attackers' computer code introduced in controlled circumstances."*

Defence tactics

- **Polymorphic techniques**: regularly changing web server code while preserving the function
- **Honey nets**: look and behave like the information resources but are actually bait that expose the attacker's actions to detailed observation
- **Dynamic execution environment** (sandbox): programs carried within network traffic first run in a quarantined environment
- **Air-gap**: physically isolate computing resources from open system networks
- **Moving target defence**: software or server instances are replaced frequently



Source: Libicki, 2015

Shift from Signature-Only to Behavior-Based Detection

Zero-day exploits

"In recognition of the limitations of signature-based analysis of network traffic (including the time lag between initial attack and availability of either a signature or a patch), defenders began to put more effort into behavioral anomaly detection.

- These approaches define normal patterns in network traffic or individual computer operations and then

- scan continuously for patterns that depart from the norm sufficiently to cause information system operators to suspect malicious activity.

These approaches escape the limitation of being able to alert only on specific signature matches, and they have the potential to discover evidence of zero-day exploits through identifying unusual behaviors."

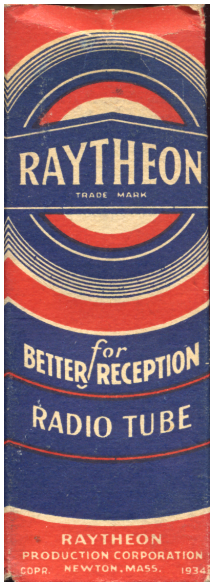
Source: Libicki, 2015

Cyber Security Operations Centre

To withstand advanced cyber threats, it is essential to have an effective Cyber Security Operations Centre – cyber situational analysis (intelligence) as a service.

Raytheon - Cyber Security Operations Centre (video)

Raytheon Tomahawk cruise missile
Source: U.S. Navy, 2002



1934

Sources

Barzilay, 2017
Menny Barzilay. A simple definition of cybersecurity. ISACA News, 2017
http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Bisson, 2016
David Bisson. People, Processes and Technology: The Triad of Your Organization's Cyber Security.
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/people-processes-and-technology-the-triad-of-your-organizations-cyber-security/

DHS, 2014
U.S. Department of Homeland Security. Cybersecurity Questions for CEOs. 2014
https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20Questions%20for%20CEOs_0.pdf

Chandola et al., 2009
Chandola, V., Banerjee, A., and Kumar, V. 2009. Anomaly detection: A survey.
ACM Computing Survey 41, 3, Article 15 (July 2009)

.

Krebs, 2015
Brian Krebs, Krebs on Security: Inside Target Corp., Days After 2013 Breach, Sept. 15, 2015
http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Libicki, 2015
Martin C. Libicki et al. The Defender's Dilemma: Charting a Course Toward Cybersecurity.
RAND Corporation, Santa Monica, CA, 2015