Cybersecurity

Dr. Uwe Glässer - Professor, Computing Science
Elnaz Mehrzadeh - Teaching Assistant, emehrzad@sfu.ca
Seyed Amir Yaghoubi Shahir - Teaching Assistant, sayaghou@sfu.ca

Perspective

- This course introduces cybersecurity and **cyber situational awareness** concepts and discusses cyber intelligence in the context of big data.
- **Cyber security analytics** and probabilistic modeling for threat detection and response (mitigative action) will play a central role.
- Coursework involves using the **R language** and software environment for statistical computing and graphics.
- Fundamental concepts and principles of **cybersecurity risk assessment**, intrusion detection and prevention, critical infrastructure protection and beyond will be discussed in detail.
- Prerequisites: CMPT 225.

Perspective (cont.)

Topics include

- Probability theory
- Discrete Markov processes
- Threat analysis and modeling
- Advanced persistent threats
- Time series analysis and forecasting
- Anomaly detection and scoring methods
- Cyber risk mitigation strategies
- Blockchain technology

Practicalities

- Office Hours

  Tuesdays, 17:00-18:00, Amir, Elnaz

  Thursdays, 16:00-17:00, Instructor

  Office hours may end after 15 minutes in case of no attendance.

- Special Sessions

  Last week of classes: 1.5 **extra hours** needed for term project presentations on DEC 2-4 and DEC 7-8, 10:00-12:00 and 14:00-16:00

- Tutorials

  R language and software environment for statistical computing

  During regular class hours as will be announced

Practicalities (cont.)

- Course Materials

  Lecture slides will be posted regularly right **after** class
  Tutorial slides will be posted regularly right **after** class
  Reading materials will be posted as needed
  No single textbook covers the entire curriculum

- Course Home Page

  https://coursys.sfu.ca/2020fa-cmpt-318-d1/pages/

- Important Dates

  Listed on the course page - updated weekly!

- Recommended Books

An Introduction to Statistical Learning: with Applications in R,
Gareth James, Daniela Witten, Trevor Hastie, and Robert Tibshirani, Springer, 2017, 978-1461471370
http://faculty.marshall.usc.edu/gareth-james/ISL/ (Not Secure!)

How to Measure Anything in Cybersecurity Risk,
Douglas W. Hubbard and Richard Seiersen, John Wiley & Sons, 2016, 978-1119085294

Grading

- Assignments (20%)

  Reading assignments

  Marked assignments

- 2 Tests (20%)

  Tests to be announced one week ahead

  Short questions with concise answers

- Term project (50%)

  …

- Class participation (10%)

  Answering questions on Piazza

  Actively engaging in discussions on Piazza

- Term Project (continued)

"One must learn by doing the thing;
for though you think you know it,
you have no certainty, until you try." —Sophocles

Working in teams of 3 team members

Technical project report (approx. 25 pages)
Project is organized in three separate parts
Who contributed what to the project needs to be documented.

Meet early and **meet often** to overcome logistic challenges.

Project teams will be finalized by next Monday.
Decide on your availability for final presentation session

Notify Amir and Elnaz by end of next week regarding your preferences!!!

Project presentation sessions (DEC 2-4 and DEC 7-8)

1. Sessions will be posted on the course page.
2. Choose a session that works for you and your team.
3. Slots will be reserved on a **first come first served** basis.

• Cybersecurity Curriculum

Joint Task Force on Cybersecurity Education

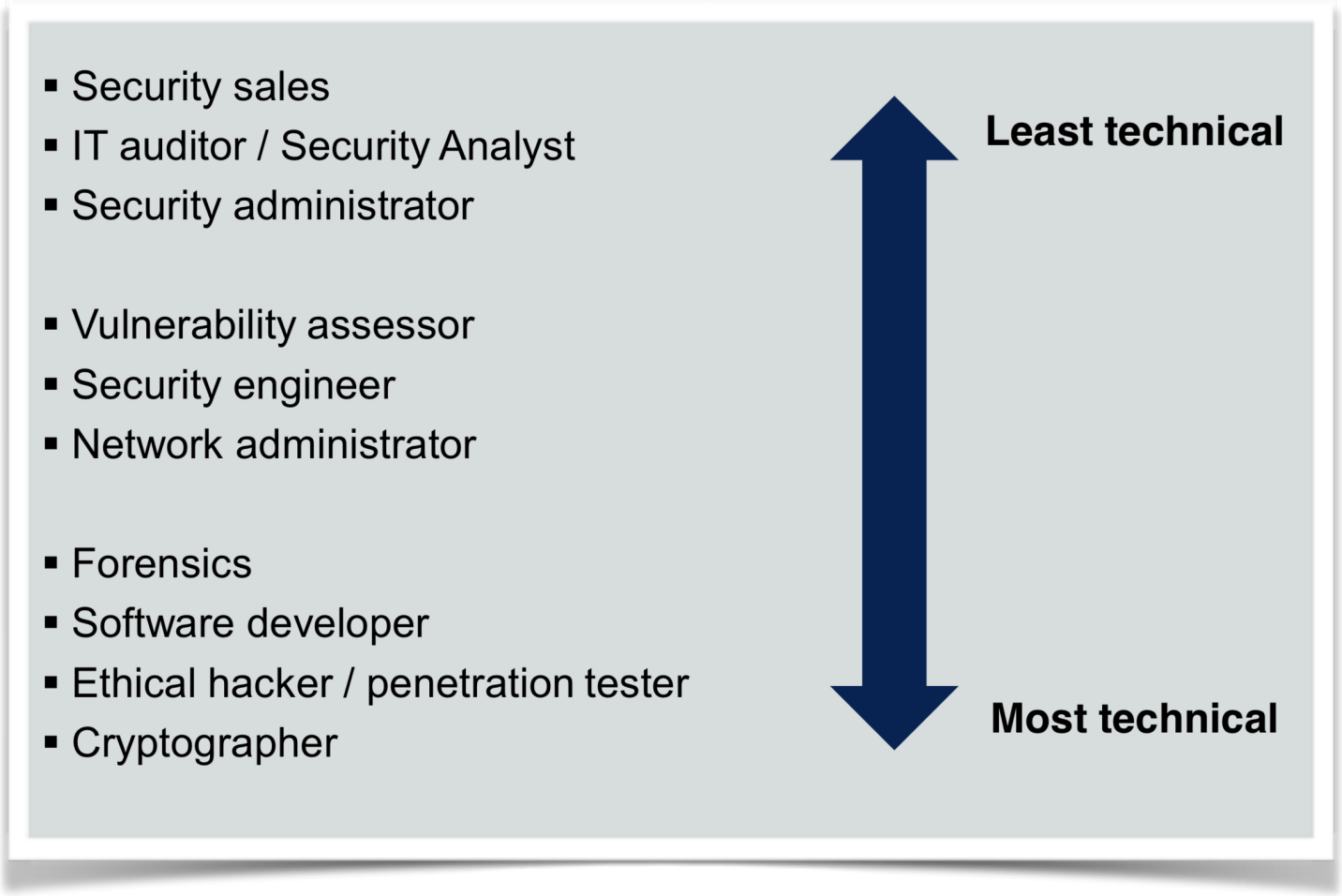
- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems (AIS)
- International Federation for Information Processing (IFIP)

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity 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."[1]

[1] While cybersecurity is an interdisciplinary course of study, it is **fundamentally a computing-based discipline**.

Career Perspectives



Source: ISACA, Vancouver

Job Market Analysis

The demand for post-secondary education in cybersecurity is steadily growing, with commercial and government sectors facing a widening gap between their needs to hire in this field and the number of skilled workforce available. Data and facts from leading analysts like Gartner and other recognized sources confirm the projected talent shortage:

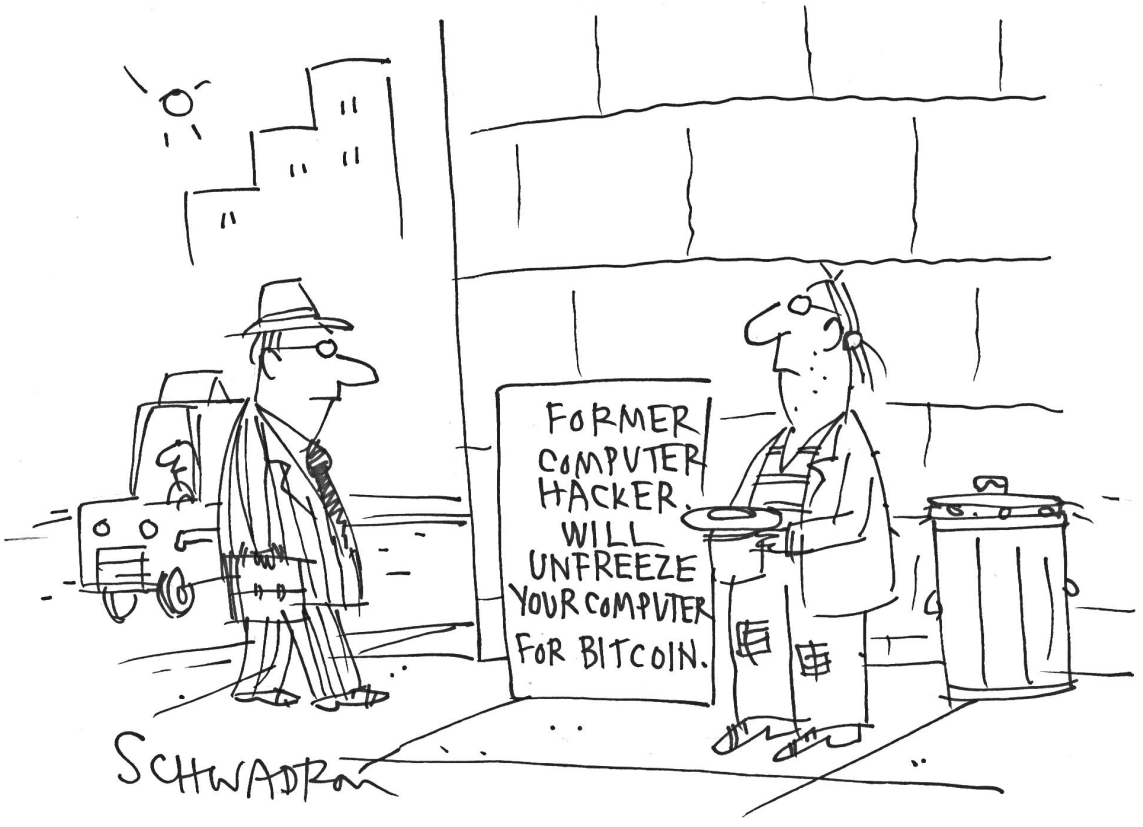
- There are currently more than **507,924** open security positions, while the total employed cybersecurity workforce is **922,720 employees** (CyberSeek, 2020).[2]

- "From June 2019 through May 2020, there were 171,000 openings for **Information Security Analysts**, but only 125,000 workers currently employed in those positions – an annual talent shortfall of 46,000 workers for cybersecurity's largest job."

  Go for it … NICE

[2] CyberSeek (2019). National Initiative for Cybersecurity Education (NICE). U.S. Department of Commerce. Retrieved from https://www.cyberseek.org/heatmap.html

SECTION 1
Cybersecurity - Introduction



Source: CartoonStock

Evolving threat landscape

Cyberattacks are increasingly routine and sophisticated—a **complex and evolving threat**. Information security breaches frequently compromise protection of sensitive data and information, exposing

- personal identities
- intellectual property
- financial assets

causing 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 attacks target critical infrastructure such as electric power grids, communication networks, and intelligent transportation networks. Beyond temporal disruption of critical services on which we all depend in our daily lives, advanced attacks can cripple vital system components physically and threaten public safety and national security beyond comprehension.[3]

[3] National Threat Assessment 2018. Canadian Centre for Cyber Security. Communications Security Establishment, October 2018.

Why do we care?

Discussion

1. What do cyber threats mean realistically?
2. Are YOU concerned personally?
3. Future impact on individuals, society and economy?

"So many of our transactions are now conducted in cyberspace that we have developed dependencies we could not even have imagined a generation ago. To be dependent is to be vulnerable. We have grown cheerfully dependent on the benefits of our online transactions, even as we observe the growth of cyber crime. We remain largely oblivious to the potential catastrophe of a well-targeted cyberattack."

— Ted Koppel, 2015

https://customernotice.lifelabs.com

An Open Letter to LifeLabs Customers

December 17, 2019

To our customers:

Through proactive surveillance, LifeLabs recently identified a cyber-attack that involved unauthorized access to our computer systems with customer information that could include name, address, email, login, passwords, date of birth, health card number and lab test results.

Personally, I want to say I am sorry that this happened. As we manage through this issue, my team and I remain focused on the best interests of our customers. You entrust us with important health information, and we take that responsibility very seriously.

We have taken several measures to protect our customer information including:

- Immediately engaging with world-class cyber security experts to isolate and secure the affected systems and determine the scope of the breach;
- Further strengthening our systems to deter future incidents;
- Retrieving the data by making a payment. We did this in collaboration with experts familiar with cyber-attacks and negotiations with cyber criminals;
- Engaging with law enforcement, who are currently investigating the matter; and
- Offering cyber security protection services to our customers, such as identity theft and fraud protection insurance.

I want to emphasize that at this time, our cyber security firms have advised that the risk to our customers in connection with this cyber-attack is low and that they have not seen any public disclosure of customer data as part of their investigations, including monitoring of the dark web and other online locations.

We have fixed the system issues related to the criminal activity and worked around the clock to put in place additional safeguards to protect your information. In the interest of transparency and as required by privacy regulations, we are making this announcement to notify all customers. There is information relating to approximately 15 million customers on the computer systems that were potentially accessed in this breach. The vast majority of these customers are in B.C. and Ontario, with relatively few customers in other locations. In the case of lab test results, our investigations to date of these systems indicate that there are 85,000 impacted customers from 2016 or earlier located in Ontario; we will be working to notify these customers directly. Our investigation to date indicates any instance of health card information was from 2016 or earlier.

While you are entitled to file a complaint with the privacy commissioners, we have already notified them of this breach and they are investigating the matter. We have also notified our government partners.

While we've been taking steps over the last several years to strengthen our cyber defenses, this has served as a reminder that we need to stay ahead of cybercrime which has become a pervasive issue around the world in all sectors.

Any customer who is concerned about this incident can receive one free year of protection that includes dark web monitoring and identity theft insurance.

Yours sincerely,

Charles Brown

President and CEO
LifeLabs

"*In 2016, the world saw cyberattacks transcend technology targets to that of wetware*—human beliefs and propensity to action. *The notion of* ***hacking democracy itself*** *came into light, posing an existential threat to entire governments and ways of life through what is sometimes known by the military as* influence operations."

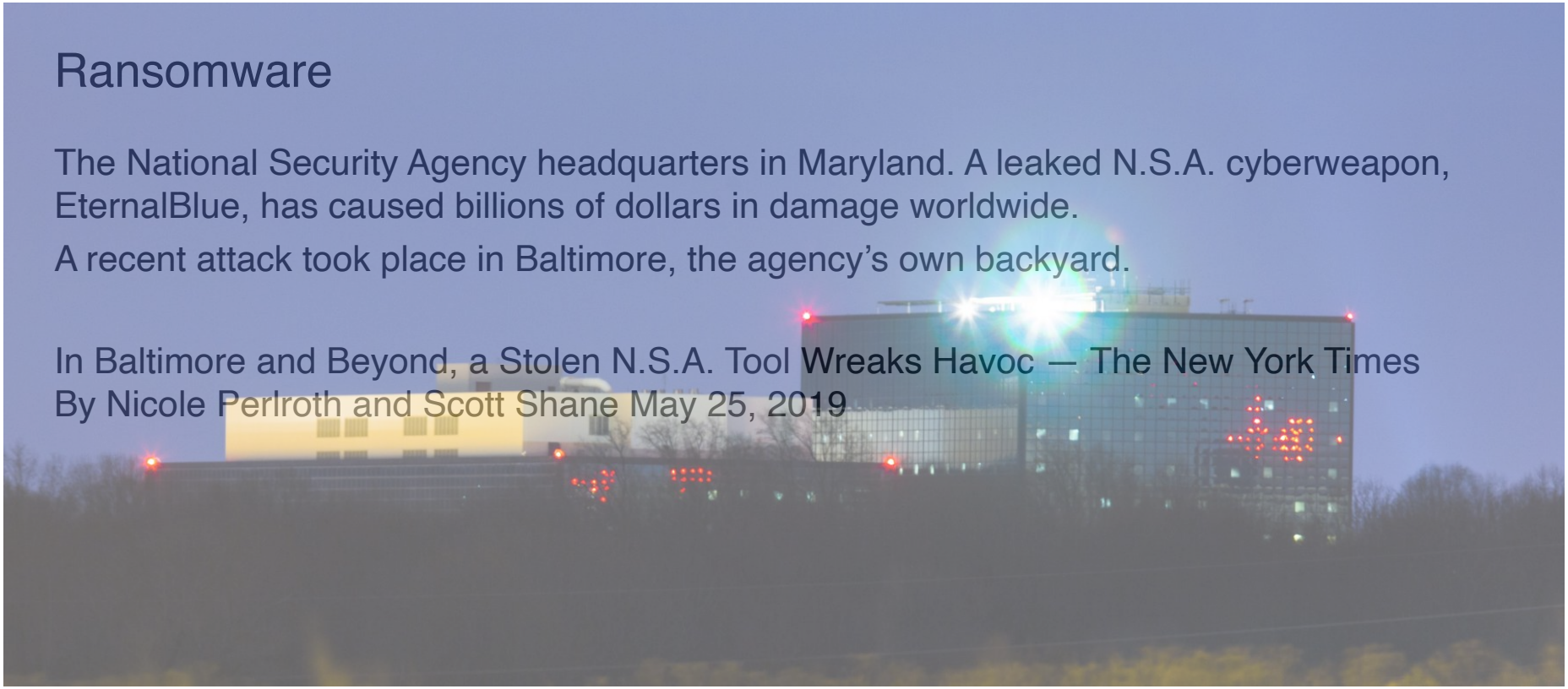
— (O. SAMI SAYDJARI, 2019)

Official Trailer (video)

Cybercrime

10 Dark Secrets of Cybercrime

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



A tale of two cities: Why ransomware will just get worse (arstechnica.com)

Texas hit by ransomware — 22 small cities took full punch (arstechnica.com, August 21)
Texas has 1,216 incorporated cities, of which only 35 have more than 100,000 residents.

Need for decisive action

Canada is one of the most connected countries in the world. Canada's security, economic prosperity and resilience in the 21st century depends upon a **safe and secure cyberspace**. The Internet and its applications are now essential to all aspects of society, creating huge opportunities as well as unforeseen threats.

National Cyber Threat Assessment 2018, Canadian Centre for Cyber Security[4] stated: "State-sponsored threat actors conduct cyber espionage **against critical infrastructure** in Canada and other allied nations. This includes reconnaissance and intelligence-gathering in the energy, aerospace and defence sectors."

[4] Communications Security Establishment (CSE) - Canada

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.

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

Source: US Homeland Security

Supervisory Control

Supervisory control is common in industrial automation for control of many individual controllers or control loops, typically within a **distributed control system** (DCS) or a **supervisory control and data acquisition** (SCADA) system.

- Automation is vital for the continuous operation of critical infrastructure and the services it provides. Electric power grids, public water utilities and smart transportation networks routinely rely on supervisory control systems, with **increasing integration of computation, networking and physical processes**.

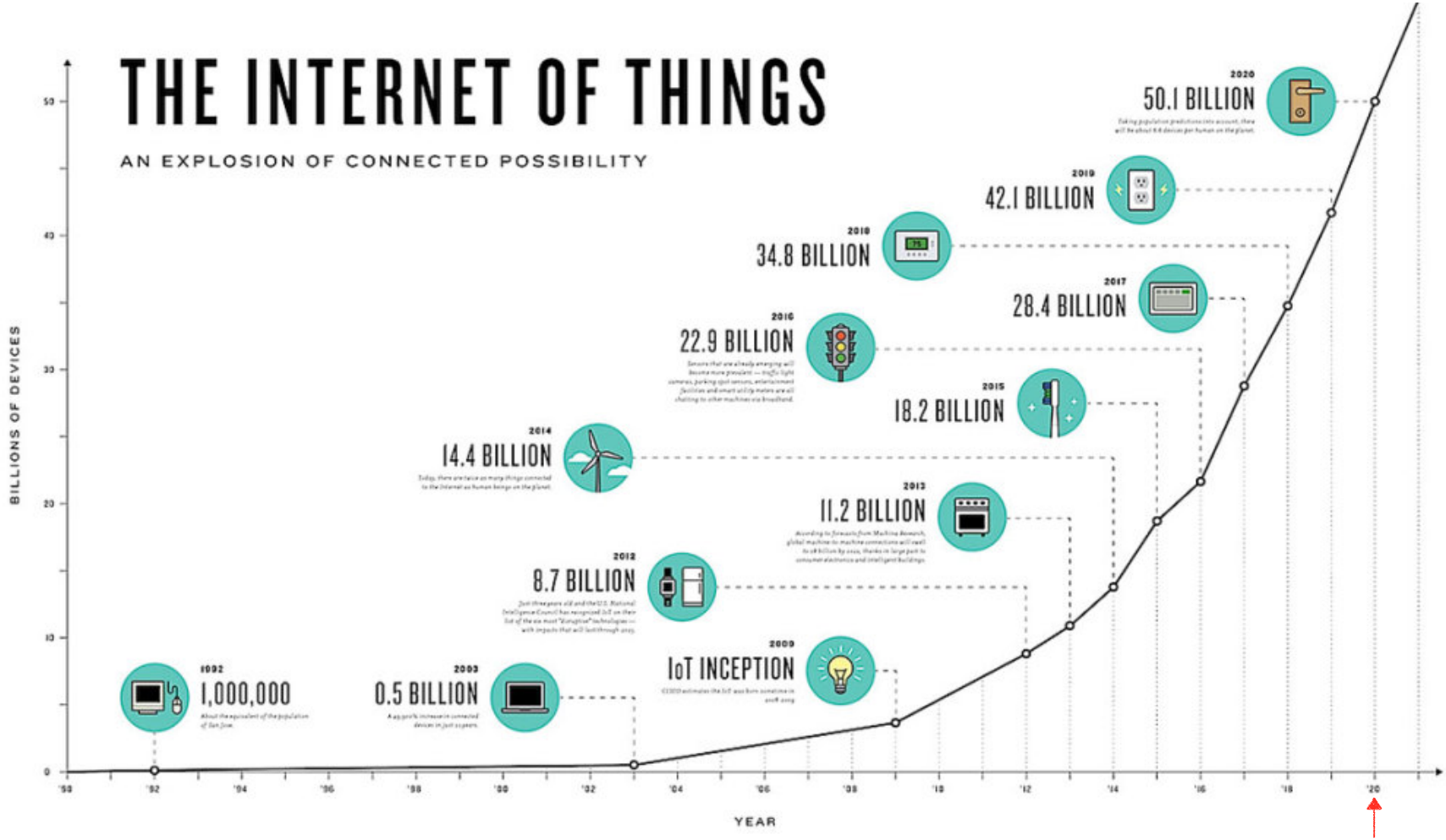
  Such systems are known as **cyber-physical systems** (CPS):

  > "Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. The technology builds on the discipline of embedded systems, computers and software embedded in **devices whose principle mission is not computation**, such as cars, toys, medical devices, and scientific instruments. CPS integrates the dynamics of the physical processes with those of the software and networking, providing abstractions and modeling, design, and analysis techniques for the integrated whole." (cyberphysicalsystems.org)

- Automation enhances cost efficiency, quality of service delivery and safe operation of critical assets. Despite the benefits, increasing reliance on automation in light of the evolving cyber threat landscape also increases the **attack surface** for advanced persistent threats and amplifies the risk of cascading effects.

  Game-changing attack targeting a *safety instrumented system* (Triconex SIS), which the targeted facility uses to prevent health- and life-threatening accidents, will serve as a **blueprint for future attacks** on other industrial systems. (arstechnica.com)

Where're we heading?



Source: Wikipedia

Here goes your privacy ...

Botnets

Mirai[5], BASHLITE and Carna

The Mirai botnet, composed primarily of embedded and IoT devices, emerged as a high-profile **distributed denial-of-service** (DDoS) threat in late 2016 when it overwhelmed several high-profile targets with massive DDoS attacks.

- Starting in September 2016, a spree of massive distributed denial-of-service (DDoS) attacks temporarily crippled Krebs on Security, OVH, and Dyn. The initial attack on Krebs **exceeded 600 Gbps in volume** — among the largest on record.
- This overwhelming traffic was sourced from hundreds of thousands of some of the Internet's least powerful hosts — Internet of Things (IoT) devices — under the control of the botnet named Mirai (Japanese for "the future").
- The botnet infected nearly 65,000 IoT devices in its first 20 hours before reaching a steady state population of 200,000– 300,000 infections.
- Mirai has spawned many variants that follow the same infection strategy, leading to speculation that "IoT botnets are the new normal of DDoS attacks."

[5] Source: Manos Antonakakis et al., Understanding the Mirai Botnet, 26th USENIX Security Symposium, 2017.

A simple definition of cybersecurity

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

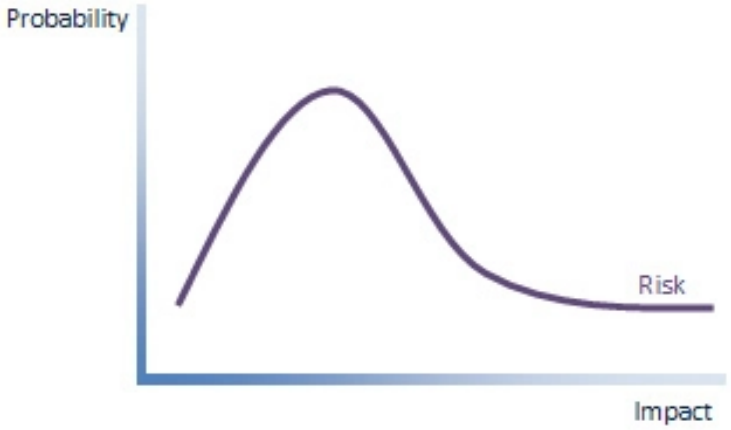


Figure 1

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

Figure 2

"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."

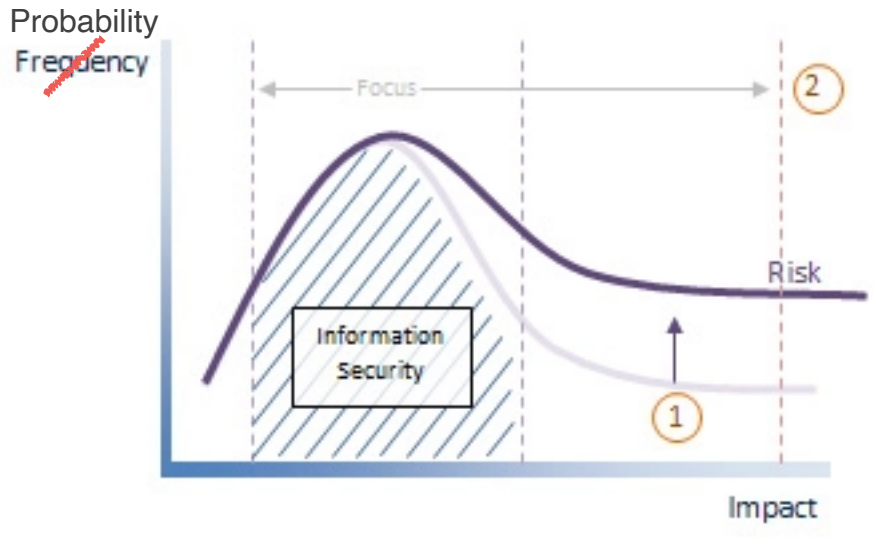


Figure 3

"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."

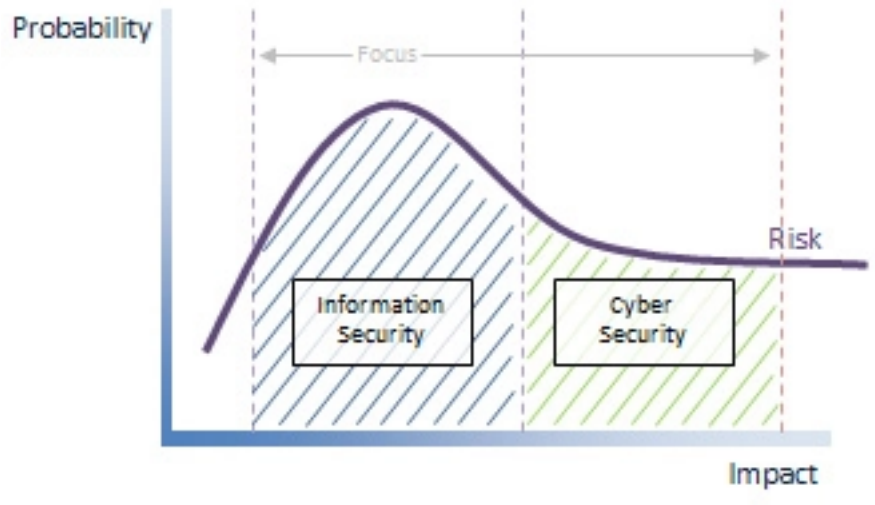


Figure 4

"This new group of very-high-impact risks that now requires our attention is commonly referred to as cyberrisk. As illustrated in Figure 4, 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**."

"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).

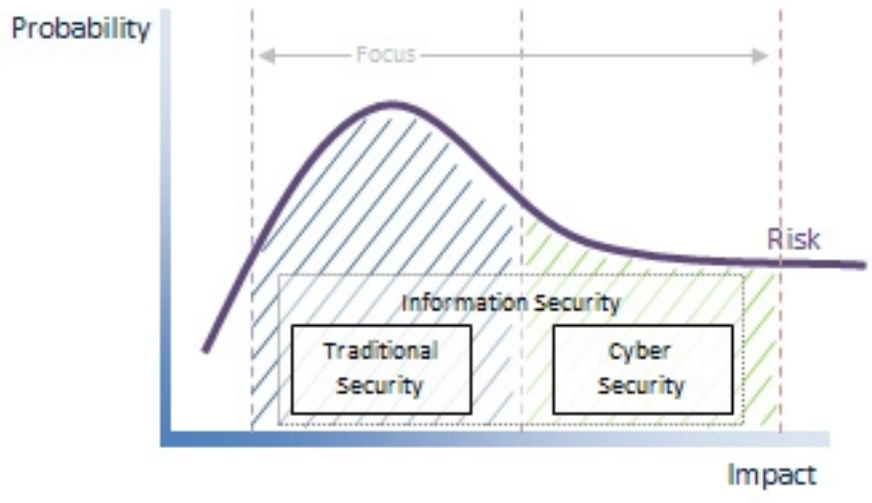


Figure 5

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, or APT, 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**:

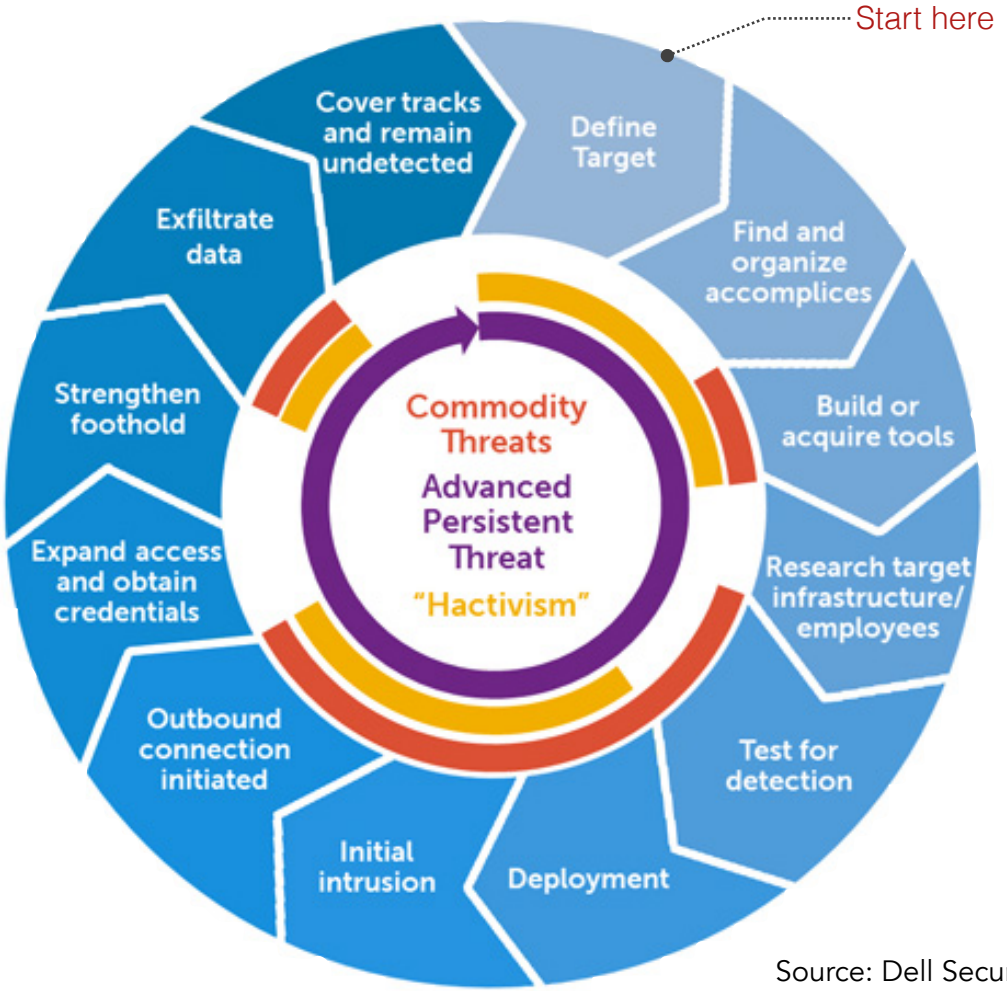
- advanced signifies sophisticated techniques using malware to exploit vulnerabilities in systems;
- persistent suggests that an external command and control system is continuously monitoring and extracting data from a specific target;
- threat indicates human involvement in orchestrating the attack.

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

This commonly refers 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 risk to organizations' financial assets, intellectual property, and reputation by following a continuous process, the kill chain.



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 social change.

Source: Dell SecureWorks

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

Inside the Cyberattack That Shocked the US Government

Brendan I. Koerner, Wired, October 23,.2016
https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

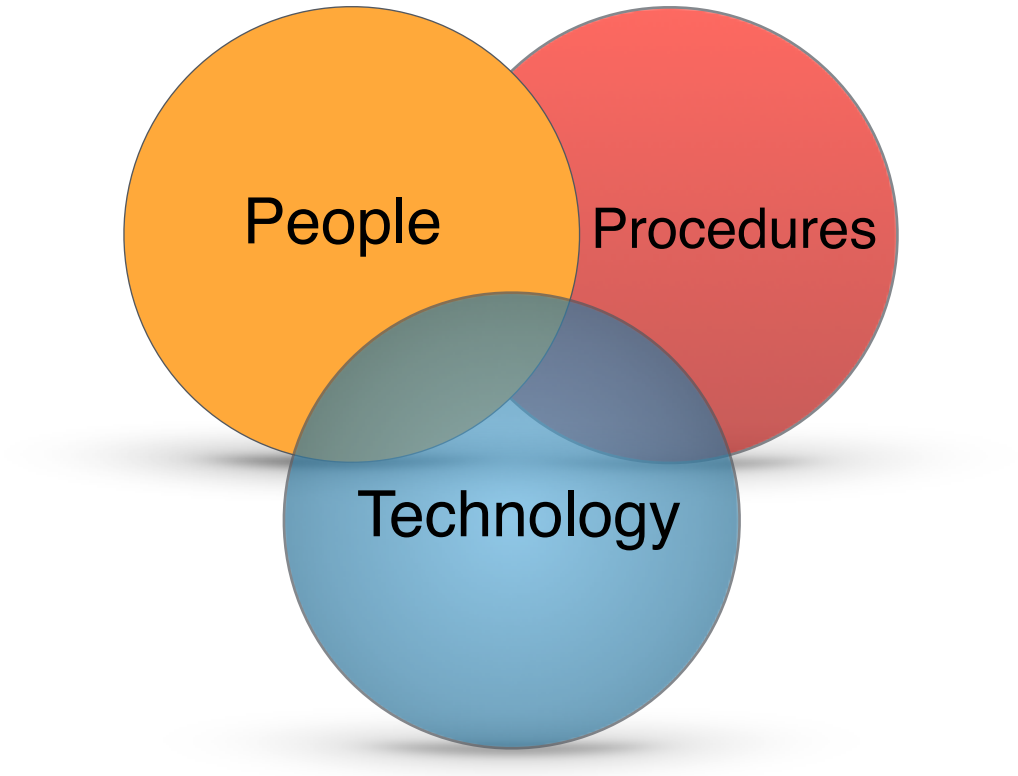
The US OFFICE of Personnel Management is the human resources department for the federal government. The agency oversees how federal employees are hired and promoted and manages benefits and pensions for millions of current and retired civil servants. The core of its own workforce, numbering well over 5,000, is headquartered in Washington, DC.

The routine nature of OPM's business made the revelations of April 15, 2015, as perplexing as they were disturbing.

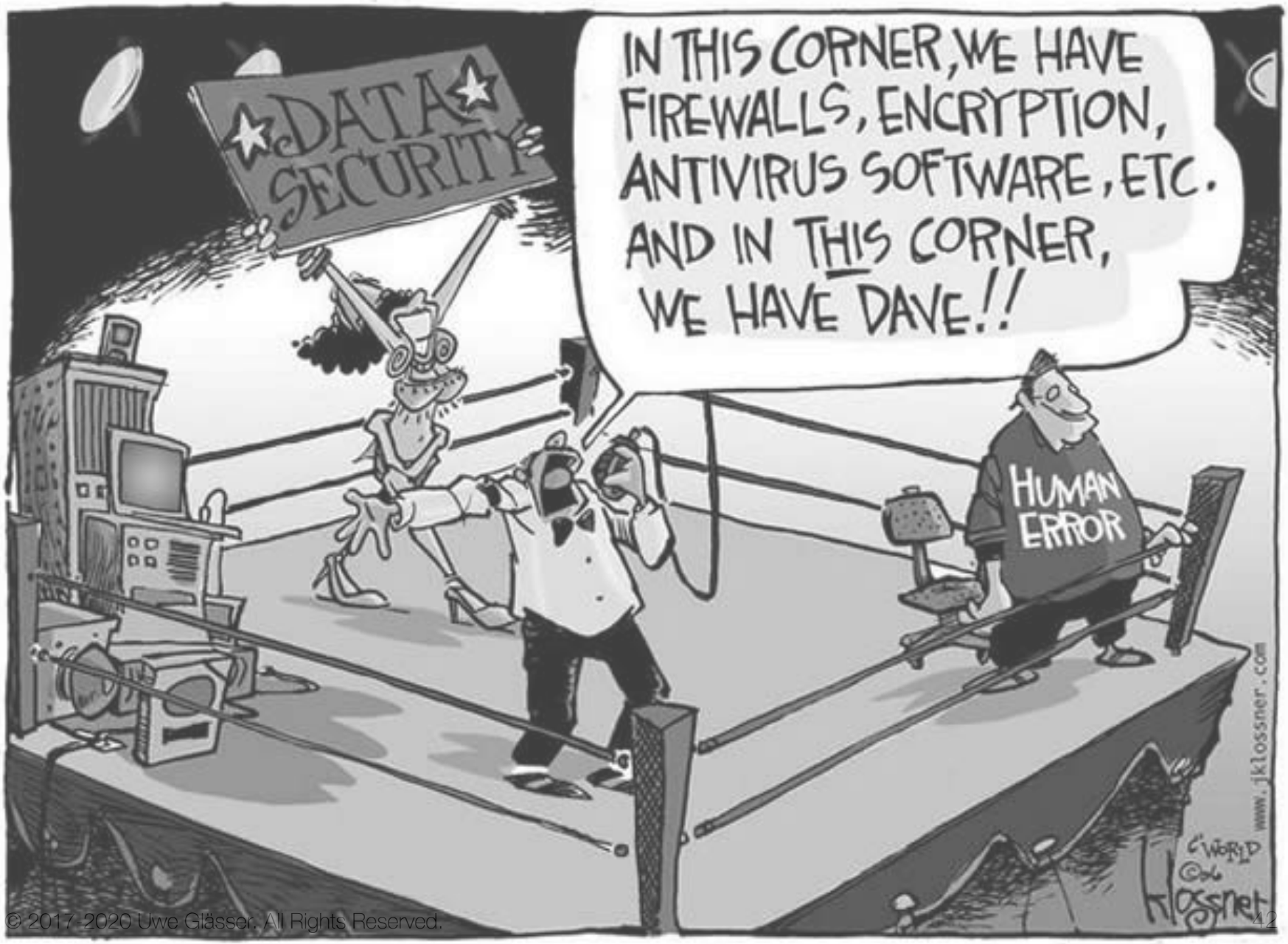
> "OPM processes over 2 million background investigations per year, involving everyone from contractors to federal judges. OPM's digital archives contain roughly **18 million copies of Standard Form 86**, a 127-page questionnaire for federal security clearance that includes probing questions about an applicant's personal finances, past substance abuse, and psychiatric care. The agency also warehouses the data that is gathered on applicants for some of the government's most secretive jobs."

Lessons learned: "We're overly focused on prevention at the expense of mitigation. One reason these attackers can do so much damage is that the average time between a malware infection and discovery of the attack is more than 200 days, a gap that has barely narrowed in recent years."

Cybersecurity Strategy



A comprehensive view of cybersecurity is critical.



The Defender's Dilemma[6]

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

> *"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

[6] 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 …

The Measure-Countermeasure Dance btw. Defender and Attacker

Measures and countermeasures to mitigate the likelihood of an attack

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

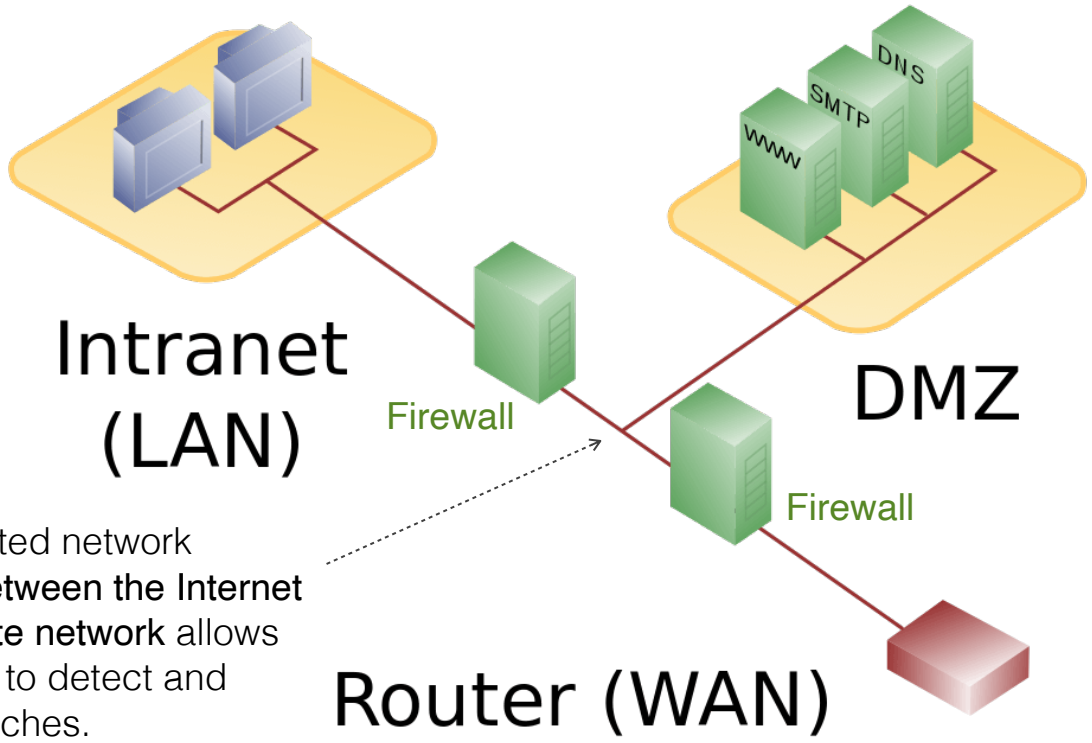
"All these approaches have to do with defenders improving the fidelity with which they identify the presence of attacker code on their systems. But there are also a class of defensive approaches that assume attackers will get through no matter what is done to stop them, reasoning that it is fundamentally 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[7] 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
- …

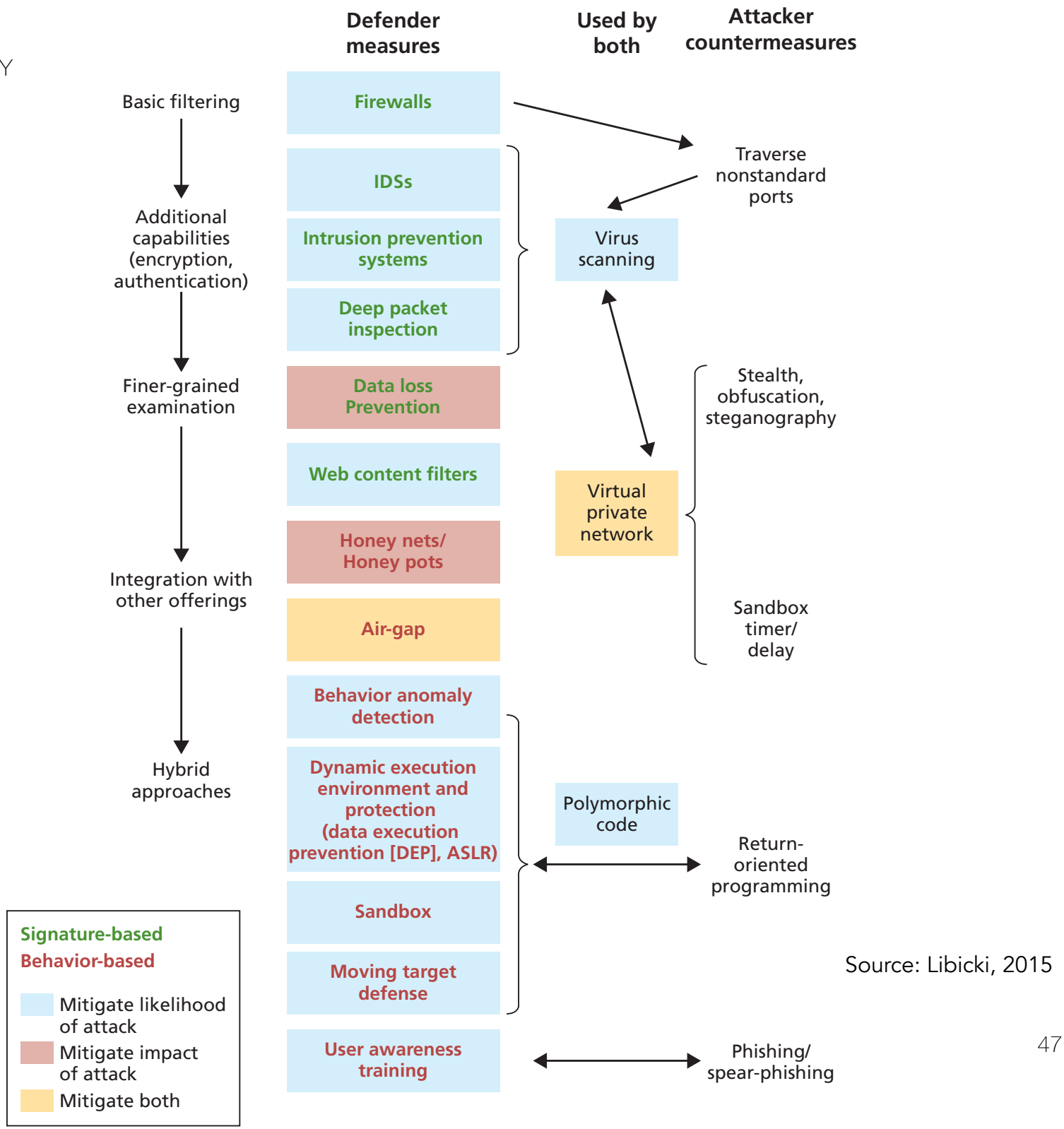
[7] **Polymorphic code** is code that uses a polymorphic engine to mutate while keeping the original algorithm intact. That is, the code changes itself each time it runs, but the function of the code will not change at all.

Demilitarized Zone



A small, isolated network positioned **between the Internet and the private network** allows for extra time to detect and address breaches.

A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a **DMZ** is to **add an additional layer of security** to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.



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.

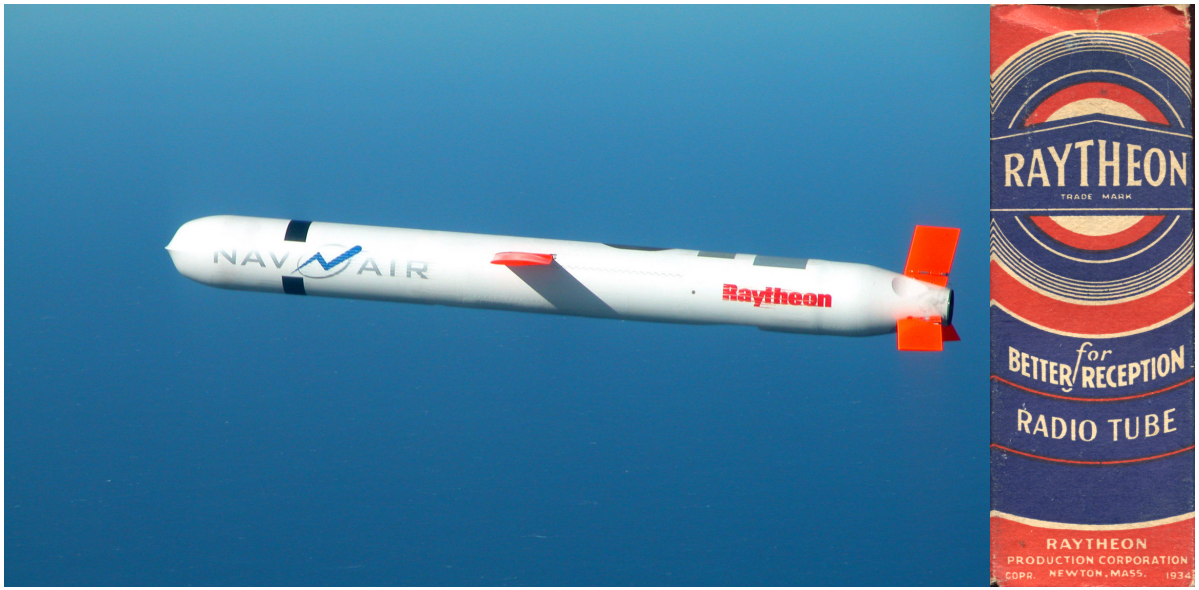
These approaches escape the limitation of being able to alert only on specific signature matches, and they have the potential to discover evidence of zero-day exploits through identifying unusual behaviors."

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 1934
Source: U.S. Navy, 2002

"Cyber security is about **risk management** at the end of the day, network technology will never be completely secure."

—Thomas Bossert[1], Cyber Week 2017

[8] Assistant to the President for Homeland Security and Counterterrorism

What exactly is cyber risk?

Conceptually, cybersecurity risk is simply the probability of cyberattacks occurring multiplied by the potential damages that would result if they actually occurred.

Estimating both of these quantities is challenging, but possible.[9]

[9] O. Sami Saydjari, Engineering Trustworthy Systems: A Principled Approach to Cybersecurity. Communications of the ACM, 62(6): 63-69, June 2019.

Threat, Vulnerability, and Risk

These three terms refer to different concepts in security. Unfortunately, they are often mixed up or used incorrectly. A clear differentiation of their meaning is important to avoid confusion. Using these terms interchangeably defeats the purpose.

Note that "risk assessment" and "threat assessment" are two entirely different things.

Assets

People, property, and information

- employees, clients and customers along with other invited persons such as contractors or guests
- tangible and intangible assets that can be assigned a value: networks, servers, intellectual property, reputation and proprietary information such as trade secrets
- databases, software code, encryption keys, critical company records, 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.

A threat, in the context of computer security, refers to anything that has **the potential** to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage.

Vulnerability

Anything that can be exploited by a threat to gain unauthorized access to an asset

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

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

Risk

Potential for loss, damage or destruction of an asset by a threat exploiting a vulnerability

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

> ... the probability of cyberattacks occurring multiplied by the potential damages that would result

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

Risk Assessment

Potential for loss, damage or destruction of an asset by 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. Understanding the difference between threats, vulnerabilities, and risk is the first step.

$$\text{Risk} = \left(\frac{\text{Vulnerability} \times \text{Threat}}{\text{Countermeasure Score}} \right) \times \text{Valuation (\$)}$$

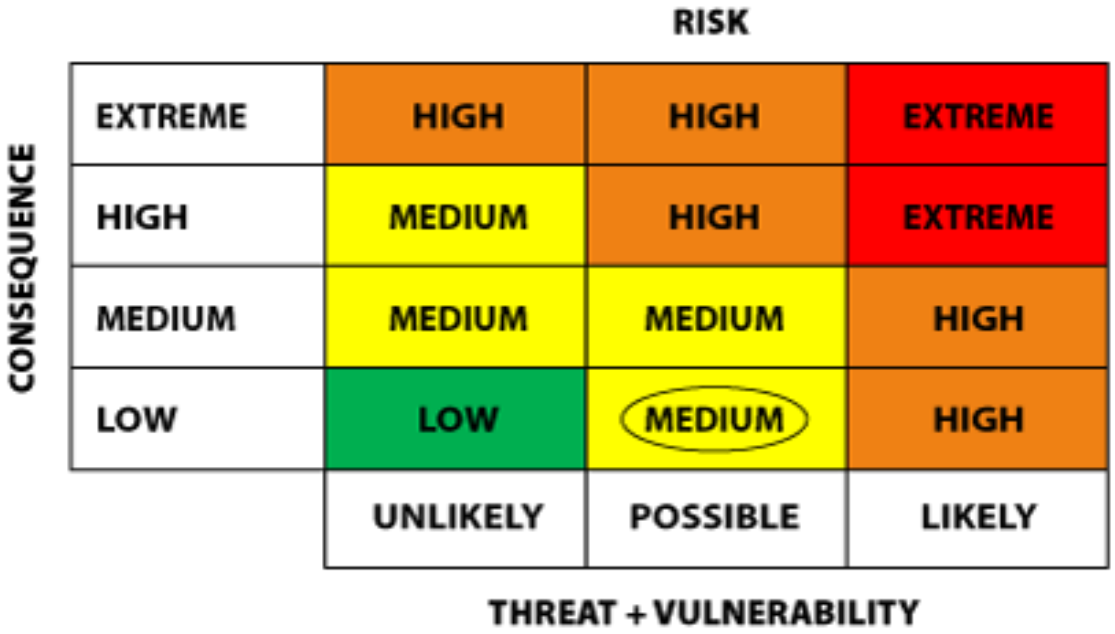
probabilistic

Risk: a function of threats exploiting vulnerabilities

Valuation: estimated value to the organization of the asset that is at risk

Countermeasures: actions we put in place to mitigate threats

A common approach to risk estimation ..



.. that may do more harm than good.

Cyber Situational Awareness[10]

Using AI to Address Advanced Threats That Last-Generation Network Security Cannot[11]

- Security teams face increased complexity and an expanded attack surface, threatening both security and network performance.
- Artificial intelligence (AI) can help in both of these areas by automating and speeding up threat detection and remediation.
- This is essential given the current landscape, as cyber criminals are using AI to create the next generation of threats.
- For network security, AI and machine learning (ML) power self-evolving detection systems (SEDS) that keep up with the evolving nature of threats and identify zero-day attacks by their characteristics.

---

[10] Gaining the situational awareness needed to mitigate cyberthreats. Industry Perspective, Splunk Inc., 2017.

[11] Fortinet. Using AI to address advanced treats that last-generation network security cannot. Jun 8, 2019.

Complexity complicates network security

A growing attack surface and increasingly complex advanced threats mean that the security controls built into “last-generation” networks are unable to address the volume, velocity, and sophistication of the threat landscape.

Traditional, signature-based antivirus can no longer keep up, as real-time detection and response is now essential.

Each day, 28% to 40% of all new malware tracked by FortiGuard Labs is zero day.[12]

Countermeasures

- AI detects zero-day threats at machine speed.
- AI is reaching a tipping point where ever-increasing CPU power allows machines to perform a wider variety of tasks **faster and more accurately than humans**. But …!
- Using ML to analyze the characteristics of malicious files, AI provides the fastest detection of advanced threats—including increasingly common zero-day attacks.

[12] Based on Fortinet internal data from FortiGuard Labs.

Countermeasures (continued)

- Automation based on AI-derived intelligence, from automatic signature creation to real-time quarantining and remediation, **represents the future of network security**.

- Unfortunately, cyber criminals are already using AI to build next-generation polymorphic malware that will spontaneously create entirely new, customized attacks.

How Machines Learn to Detect Malware

It takes a lot of capacity and data for SEDS to work properly. Large ANNs—systems of hardware and/or software patterned after the operation of neurons in the human brain—are required to collect, analyze, and classify millions of threats every day. "Training" of AI algorithms involves **three different types of learning**:

1. *Supervised Learning:* Presenting the system with correctly labeled data, which it analyzes and applies to unlabeled data.

2. *Unsupervised Learning*: Providing unknown solution sets, which the system analyzes for patterns from which it can ultimately label the data.

3. *Reinforcement Learning*: Optimizing the system's performance by testing it with unlabeled data and offering grades (rewards) for the results.

Comprehensive training over a period of time **results in billions of examples** that are subjected to extensive analysis for features and behaviors that suggest whether a file is clean or malicious. The result is **instantaneous decisions** that reflect a high degree of accuracy—enabling remediation in real time.

Concluding

"Make no mistake: The future of cybersecurity is about embracing and innovating for the partnership of man and machine—both relying on each other in the fight against hackers."[13]

[13] Laurent Gil, "The Debate is Over: Artificial Intelligence is the Future for Cybersecurity," SC Magazine, March 22, 2018.

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/

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)

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
.
Kroerner, 2016
Brendan I. Koerner, Inside the Cyberattack That Shocked the US Government, Wired, October 23, 2016,
https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

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/

Sources (cont.)

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

Saydjari, 2019
O. Sami Saydjari, Engineering Trustworthy Systems: A Principled Approach to Cybersecurity. Communications of the ACM, 62(6): 63-69, June 2019.