Computer security

Computer security, **cybersecurity** (**cyber security**), or **information technology security** (**IT security**) is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.[1][2]

The field has become of significance due to the expanded reliance on computer systems, the Internet,[3] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is also one of the significant challenges in the contemporary world, due to the complexity of information systems, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy.[4][5]

While most aspects of computer security involve digital measures such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering.

Contents

History

Since the Internet's arrival and with the digital transformation initiated in recent years, the notion of cybersecurity has become a familiar subject in both our professional and personal lives. Cybersecurity and cyber threats have been consistently present for the last 50 years of technological change. In the 1970s and 1980s, computer security was mainly limited to academia until the conception of the Internet, where, with increased connectivity, computer viruses and network intrusions began to take off. After the spread of viruses in the 1990s, the 2000s marked the institutionalization of cyber threats and cybersecurity.

The April 1967 session organized by Willis Ware at the Spring Joint Computer Conference, and the later publication of the Ware Report, were foundational moments in the history of the field of computer security.[6] Ware's work straddled the intersection of material, cultural, political, and social concerns.[6]

A 1977 NIST publication[7] introduced the "CIA triad" of Confidentiality, Integrity, and Availability as a clear and simple way to describe key security goals.[8] While still relevant, many more elaborate frameworks have since been proposed.[9][10]

However, in the 1970s and 1980s there were no grave computer threats because computers and the internet were still developing, and security threats were easily identifiable. Most often, threats came from malicious insiders who gained unauthorized access to sensitive documents and files. Although malware and network breaches existed during the early years, they did not use them for financial gain. By the second half of the 1970s, established computer firms like IBM started offering commercial access control systems and computer security software products.[11]

It started with **Creeper** in 1971. Creeper was an experimental computer program written by Bob Thomas at BBN. It is considered the first computer worm. In 1972, the first anti-virus software was created, called **Reaper**. It was created by Ray Tomlinson to move across the ARPANET and delete the Creeper worm.

Between September 1986 and June 1987, a group of German hackers performed the first documented case of cyber espionage. The group hacked into American defense contractors, universities, and military bases' networks and sold gathered information to the Soviet KGB. The group was led by Markus Hess, who was arrested on 29 June 1987. He was convicted of espionage (along with two co-conspirators) on 15 Feb 1990.

In 1988, one of the first computer worms, called the Morris worm, was distributed via the Internet. It gained significant mainstream media attention.

In 1993, Netscape started developing the protocol SSL, shortly after the National Center for Supercomputing Applications (NCSA) launched Mosaic 1.0, the first web browser, in 1993. Netscape had SSL version 1.0 ready in 1994, but it was never released to the public due to many serious security vulnerabilities. These weaknesses included replay attacks and a vulnerability that allowed hackers to alter unencrypted communications sent by users. However, in February 1995, Netscape launched the Version 2.0.

Failed offensive strategy

The National Security Agency (NSA) is responsible for the protection of U.S. information systems and also for collecting foreign intelligence.[12] These two duties are in conflict with each other. Protecting information systems includes evaluating software, identifying security flaws, and taking steps to correct the flaws, which is a defensive action. Collecting intelligence includes exploiting security flaws to extract information, which is an offensive action. Correcting security flaws makes the flaws unavailable for NSA exploitation.

The agency analyzes commonly used software in order to find security flaws, which it reserves for offensive purposes against competitors of the United States. The agency seldom takes defensive action by reporting the flaws to software producers so that they can eliminate them.[13]

The offensive strategy worked for a while, but eventually other nations, including Russia, Iran, North Korea, and China, acquired their own offensive capability and have tended to use it against the United States. NSA contractors created and sold "click-and-shoot" attack tools to U.S. agencies and close allies, but eventually the tools made their way to foreign adversaries. In 2016, NSAs own hacking tools were hacked, and they have been used by Russia and North Korea. NSA's employees and contractors have been recruited at high salaries by adversaries, anxious to compete in cyberwarfare.[13]

For example, in 2007, the United States and Israel began exploiting security flaws in the Microsoft Windows operating system to attack and damage equipment used in Iran to refine nuclear materials. Iran responded by heavily investing in their own cyberwarfare capability, which they began using against the United States.[13]

Vulnerabilities and attacks

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An *exploitable* vulnerability is one for which at least one working attack or *exploit*

exists.[14] Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts.[15][16] To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of these categories below:

Backdoor

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for many reasons, including by original design or poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Backdoors can be very hard to detect, and backdoors are usually discovered by someone who has access to application source code or intimate knowledge of the operating system of the computer.

Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.[17] Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless microphones. Even when the system is protected by standard security measures, these may be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

Eavesdropping

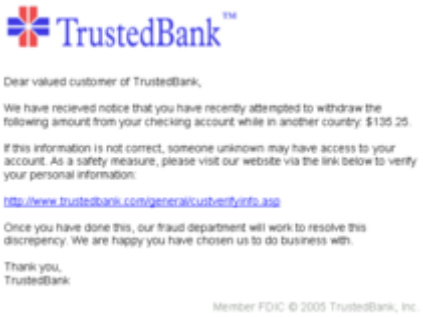
Eavesdropping is the act of surreptitiously listening to a private computer "conversation" (communication), typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the Federal Bureau of Investigation (FBI) and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

Multi-vector, polymorphic attacks

Surfacing in 2017, a new class of multi-vector,[18] polymorphic[19] cyber threats combined several types of attacks and changed form to avoid cybersecurity controls as they spread.

Phishing

Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users.[20] Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose "look" and "feel" are almost identical to the legitimate one. The fake website often asks for personal information, such as log-in details and passwords. This information can then be used to gain access to the individual's real account on the real website. Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers are using creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices[21] to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

An example of a phishing email, disguised as an official email from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website. Note the misspelling of the words *received* and *discrepancy* as *recieved* and *discrepency*, respectively. Although the URL of the bank's webpage appears to be legitimate, the hyperlink points at the phisher's webpage.

Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to exploit a vulnerability in the system to gain access to restricted data; or even become "root" and have full unrestricted access to a system.

Reverse engineering

Reverse engineering is the process by which a man-made object is deconstructed to reveal its designs, code, architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon.[22]:3

Side-channel attack

Any computational system affects its environment in some form. This effect it has on its environment, includes a wide range of criteria, which can range from electromagnetic radiation, to residual effect on RAM cells which as a consequent make a Cold boot attack possible, to hardware implementation faults which allow for access and or guessing of other values that normally should be inaccessible. In Side-channel attack scenarios the attacker would gather such information about a system or network to guess its internal state, and as a result access the information which is assumed by the victim to be secure.

Social engineering

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access by, for example, impersonating a senior executive, bank, a contractor, or a customer.[23] This generally involves exploiting peoples trust, and relying on their cognitive biases. A common scam involves emails sent to accounting and finance department personnel,

impersonating their CEO and urgently requesting some action. In early 2016, the FBI reported that such "business email compromise" (BEC) scams had cost US businesses more than $2 billion in about two years.[24]

In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.[25]

Spoofing

Spoofing is an act of masquerading as a valid entity through falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain.[26][27] There are several types of spoofing, including:

- Email spoofing, is where an attacker forges the sending (*From*, or source) address of an email.
- IP address spoofing, where an attacker alters the source IP address in a network packet to hide their identity or impersonate another computing system.
- MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of their network interface controller to obscure their identity, or to pose as another.
- Biometric spoofing, where an attacker produces a fake biometric sample to pose as another user.[28]

Tampering

Tampering describes a malicious modification or alteration of data. So-called Evil Maid attacks and security services planting of surveillance capability into routers are examples.[29]

Malware

Malicious software (malware) installed on a computer can leak any information, such as personal information, business information and passwords, can give control of the system to the attacker, and can corrupt or delete data permanently.[30]

Information security culture

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. Information security culture is the "...totality of patterns of behavior in an organization that contributes to the protection of information of all kinds."[31]

Andersson and Reimers (2014) found that employees often do not see themselves as part of their organization's information security effort and often take actions that impede organizational changes.[32] Indeed, the Verizon Data Breach Investigations Report 2020, which examined 3,950 security breaches, discovered 30% of cyber security incidents involved internal actors within a company.[33] Research shows information security culture needs to be improved continuously. In ″Information Security Culture from

Analysis to Change", authors commented, "It's a never-ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.[34]

- Pre-evaluation: To identify the awareness of information security within employees and to analyze the current security policies.
- Strategic planning: To come up with a better awareness program, clear targets need to be set. Assembling a team of skilled professionals is helpful to achieve it.
- Operative planning: A good security culture can be established based on internal communication, management-buy-in, security awareness and a training program.[34]
- Implementation: Four stages should be used to implement the information security culture. They are:

    1. Commitment of the management
    2. Communication with organizational members
    3. Courses for all organizational members
    4. Commitment of the employees[34]

- Post-evaluation: To assess the success of the planning and implementation, and to identify unresolved areas of concern.

Systems at risk

The growth in the number of computer systems and the increasing reliance upon them by individuals, businesses, industries, and governments means that there are an increasing number of systems at risk.

Financial systems

The computer systems of financial regulators and financial institutions like the U.S. Securities and Exchange Commission, SWIFT, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested in manipulating markets and making illicit gains.[35] Websites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are also prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market.[36] In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.[37]

Aviation

The aviation industry is very reliant on a series of complex systems which could be attacked.[38] A simple power outage at one airport can cause repercussions worldwide,[39] much of the system relies on radio transmissions which could be disrupted,[40] and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore.[41] There is also potential for attack from within an aircraft.[42]

In Europe, with the (Pan-European Network Service)[43] and NewPENS,[44] and in the US with the NextGen program,[45] air navigation service providers are moving to create their own dedicated networks.

The consequences of a successful attack range from loss of confidentiality to loss of system integrity, air traffic control outages, loss of aircraft, and even loss of life.

Consumer devices

Desktop computers and laptops are commonly targeted to gather passwords or financial account information, or to construct a botnet to attack another target. Smartphones, tablet computers, smart watches, and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. WiFi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.[46]

The increasing number of home automation devices such as the Nest thermostat are also potential targets.[46]

Large corporations

Large corporations are common targets. In many cases attacks are aimed at financial gain through identity theft and involve data breaches. Examples include the loss of millions of clients' credit card details by Home Depot,[47] Staples,[48] Target Corporation,[49] and the most recent breach of Equifax.[50]

Medical records have been targeted in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale.[51] Although cyber threats continue to increase, 62% of all organizations did not increase security training for their business in 2015.[52]

Not all attacks are financially motivated, however: security firm HBGary Federal suffered a serious series of attacks in 2011 from hacktivist group Anonymous in retaliation for the firm's CEO claiming to have infiltrated their group,[53][54] and Sony Pictures was hacked in 2014 with the apparent dual motive of embarrassing the company through data leaks and crippling the company by wiping workstations and servers.[55][56]

Automobiles

Vehicles are increasingly computerized, with engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver-assistance systems on many models. Additionally, connected cars may use WiFi and Bluetooth to communicate with onboard consumer devices and the cell phone network.[57] Self-driving cars are expected to be even more complex. All of these systems carry some security risk, and such issues have gained wide attention.[58][59][60]

Simple examples of risk include a malicious compact disc being used as an attack vector,[61] and the car's onboard microphones being used for eavesdropping. However, if access is gained to a car's internal controller area network, the danger is much greater[57] – and in a widely publicized 2015 test, hackers remotely carjacked a vehicle from 10 miles away and drove it into a ditch.[62][63]

Manufacturers are reacting in numerous ways, with Tesla in 2016 pushing out some security fixes "over the air" into its cars' computer systems.[64] In the area of autonomous vehicles, in September 2016 the United States Department of Transportation announced some initial safety standards, and called for states to come up with uniform policies.[65][66]

Government

Government and military computer systems are commonly attacked by activists[67][68][69] and foreign powers.[70][71][72][73] Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records,[74] and financial systems are also potential targets as they are now all largely computerized. Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning.

Internet of things and physical vulnerabilities

The Internet of things (IoT) is the network of physical objects such as devices, vehicles, and buildings that are embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data.[75] Concerns have been raised that this is being developed without appropriate consideration of the security challenges involved.[76][77]

While the IoT creates opportunities for more direct integration of the physical world into computer-based systems,[78][79] it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyberattacks are likely to become an increasingly physical (rather than simply virtual) threat.[80] If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-Internet-connected hotel door locks.[81]

An attack that targets physical infrastructure and/or human lives is sometimes referred to as a cyber-kinetic attack. As IoT devices and appliances gain currency, cyber-kinetic attacks can become pervasive and significantly damaging.

Medical systems

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment[82] and implanted devices including pacemakers[83] and insulin pumps.[84] There are many reports of hospitals and hospital organizations getting hacked, including ransomware attacks,[85][86][87][88] Windows XP exploits,[89][90] viruses,[91][92] and data breaches of sensitive data stored on hospital servers.[93][86][94][95] On 28 December 2016 the US Food and Drug Administration released its recommendations for how medical device manufacturers should maintain the security of Internet-connected devices – but no structure for enforcement.[96][97]

Energy sector

In distributed generation systems, the risk of a cyber attack is real, according to *Daily Energy Insider*. An attack could cause a loss of power in a large area for a long period of time, and such an attack could have just as severe consequences as a natural disaster. The District of Columbia is considering creating a Distributed Energy Resources (DER) Authority within the city, with the goal being for customers to have more insight into their own energy use and giving the local electric utility, Pepco, the chance to better estimate energy demand. The D.C. proposal, however, would "allow third-party vendors to create numerous points of energy distribution, which could potentially create more opportunities for cyber attackers to threaten the electric grid."[98]

Impact of security breaches

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. "Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal."[99]

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic Gordon-Loeb Model analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the expected value of the loss resulting from a cyber/information security breach).[100]

Attacker motivation

As with physical security, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists, others are criminals looking for financial gain. State-sponsored attackers are now common and well resourced but started with amateurs such as Markus Hess who hacked for the KGB, as recounted by Clifford Stoll in *The Cuckoo's Egg*.

Additionally, recent attacker motivations can be traced back to extremist organizations seeking to gain political advantage or disrupt social agendas.[101] The growth of the internet, mobile technologies, and inexpensive computing devices have led to a rise in capabilities but also to the risk to environments that are deemed as vital to operations. All critical targeted environments are susceptible to compromise and this has led to a series of proactive studies on how to migrate the risk by taking into consideration motivations by these types of actors. Several stark differences exist between the hacker motivation and that of nation state actors seeking to attack based on an ideological preference.[102]

A standard part of threat modeling for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level and detail of precautions will vary depending on the system to be secured. A home personal computer, bank, and classified military network face very different threats, even when the underlying technologies in use are similar.[103]

Computer protection (countermeasures)

In computer security, a countermeasure is an action, device, procedure or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.[104][105][106]

Some common countermeasures are listed in the following sections:

Security by design

Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way, even if an attacker gains access to that part, they only have limited access to the whole system.
- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing, approaches to make modules more secure where formal correctness proofs are not possible.
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
- Default secure settings, and design to "fail secure" rather than "fail insecure" (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
- Audit trails track system activity so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.
- Full disclosure of all vulnerabilities, to ensure that the *window of vulnerability* is kept as short as possible when bugs are discovered.

Security architecture

The Open Security Architecture organization defines IT security architecture as "the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services".[107]

Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are:[108]

- the relationship of different components and how they depend on each other.
- determination of controls based on risk assessment, good practices, finances, and legal matters.
- the standardization of controls.

Practicing security architecture provides the right foundation to systematically address business, IT and security concerns in an organization.

Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware and software-based.
- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, the complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security consists mainly of "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real-time filtering and blocking. Another implementation is a so-called "physical firewall", which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

Some organizations are turning to big data platforms, such as Apache Hadoop, to extend data accessibility and machine learning to detect advanced persistent threats.[109]

However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As a result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets".[110] The primary obstacle to effective eradication of cybercrime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

In order to ensure adequate security, the confidentiality, integrity and availability of a network, better known as the CIA triad, must be protected and is considered the foundation to information security.[111] To achieve those objectives, administrative, physical and technical security measures should be employed. The amount of security afforded to an asset can only be determined when its value is known.[112]

Vulnerability management

Vulnerability management is the cycle of identifying, remediating or mitigating vulnerabilities,[113] especially in software and firmware. Vulnerability management is integral to computer security and network security.

Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities,[114] such as open ports, insecure software configuration, and susceptibility to malware. In order for these tools to be effective, they must be kept up to date with every new update the vendor release. Typically, these updates will scan for the new vulnerabilities that were introduced recently.

Beyond vulnerability scanning, many organizations contract outside security auditors to run regular penetration tests against their systems to identify vulnerabilities. In some sectors, this is a contractual requirement.[115]

Reducing vulnerabilities

While formal verification of the correctness of computer systems is possible,[116][117] it is not yet common. Operating systems formally verified include seL4,[118] and SYSGO's PikeOS[119][120] – but these make up a very small percentage of the market.

Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or another piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk, but even in highly disciplined environments (e.g. military organizations), social engineering attacks can still be difficult to foresee and prevent.

Inoculation, derived from inoculation theory, seeks to prevent social engineering and other fraudulent tricks or traps by instilling a resistance to persuasion attempts through exposure to similar or related attempts.[121]

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner and/or hiring people with expertise in security, though none of these guarantee the prevention of an attack. The effects of data loss/damage can be reduced by careful backing up and insurance.

Hardware protection mechanisms

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process,[122][123] hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below.

- USB dongles are typically used in software licensing schemes to unlock software capabilities, but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs).[124] In addition, a USB dongle can be configured to lock or unlock a computer.[125]
- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.[126]

- Computer case intrusion detection refers to a device, typically a push-button switch, which detects when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.[127] Tools exist specifically for encrypting external drives as well.[128]
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.
- Disconnecting or disabling peripheral devices (like camera, GPS, removable storage etc.), that are not in use.[129]
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), near-field communication (NFC) on non-iOS devices and biometric validation such as thumbprint readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.[130]

Secure operating systems

One use of the term "computer security" refers to technology that is used to implement secure operating systems. In the 1980s, the United States Department of Defense (DoD) used the "Orange Book"[131] standards, but the current international standard ISO/IEC 15408, "Common Criteria" defines a number of progressively more stringent Evaluation Assurance Levels. Many common operating systems meet the EAL4 standard of being "Methodically Designed, Tested and Reviewed", but the formal verification required for the highest levels means that they are uncommon. An example of an EAL6 ("Semiformally Verified Design and Tested") system is INTEGRITY-178B, which is used in the Airbus A380[132] and several military jets.[133]

Secure coding

In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are *secure by design*. Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system;[134] important for cryptographic protocols for example.

Capabilities and access control lists

Within computer systems, two of the main security models capable of enforcing privilege separation are access control lists (ACLs) and role-based access control (RBAC).

An access-control list (ACL), with respect to a computer file system, is a list of permissions associated with an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

Role-based access control is an approach to restricting system access to authorized users,[135][136][137] used by the majority of enterprises with more than 500 employees,[138] and can implement mandatory access control (MAC) or discretionary access control (DAC).

A further approach, capability-based security has been mostly restricted to research operating systems. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open-source project in the area is the E language.

End user security training

The end-user is widely recognized as the weakest link in the security chain[139] and it is estimated that more than 90% of security incidents and breaches involve some kind of human error.[140][141] Among the most commonly recorded forms of errors and misjudgment are poor password management, sending emails containing sensitive data and attachments to the wrong recipient, the inability to recognize misleading URLs and to identify fake websites and dangerous email attachments. A common mistake that users make is saving their user id/password in their browsers to make it easier to log in to banking sites. This is a gift to attackers who have obtained access to a machine by some means. The risk may be mitigated by the use of two-factor authentication.[142]

As the human component of cyber risk is particularly relevant in determining the global cyber risk[143] an organization is facing, security awareness training, at all levels, not only provides formal compliance with regulatory and industry mandates but is considered essential[144] in reducing cyber risk and protecting individuals and companies from the great majority of cyber threats.

The focus on the end-user represents a profound cultural change for many security practitioners, who have traditionally approached cybersecurity exclusively from a technical perspective, and moves along the lines suggested by major security centers[145] to develop a culture of cyber awareness within the organization, recognizing that a security-aware user provides an important line of defense against cyber attacks.

Digital hygiene

Related to end-user training, **digital hygiene** or **cyber hygiene** is a fundamental principle relating to information security and, as the analogy with personal hygiene shows, is the equivalent of establishing simple routine measures to minimize the risks from cyber threats. The assumption is that good cyber hygiene practices can give networked users another layer of protection, reducing the risk that one vulnerable node will be used to either mount attacks or compromise another node or network, especially from common cyberattacks.[146] Cyber hygiene should also not be mistaken for proactive cyber defence, a military term.[147]

As opposed to a purely technology-based defense against threats, cyber hygiene mostly regards routine measures that are technically simple to implement and mostly dependent on discipline[148] or education.[149] It can be thought of as an abstract list of tips or measures that have been demonstrated as having a positive effect on personal and/or collective digital security. As such, these measures can be performed by laypeople, not just security experts.

Cyber hygiene relates to personal hygiene as computer viruses relate to biological viruses (or pathogens). However, while the term *computer virus* was coined almost simultaneously with the creation of the first working computer viruses,[150] the term *cyber hygiene* is a much later invention, perhaps as late as 2000[151] by Internet pioneer Vint Cerf. It has since been adopted by the Congress[152] and Senate of the United States,[153] the FBI,[154] EU institutions[146] and heads of state.[147]

Response to breaches

Responding to attempted security breaches is often very difficult for a variety of reasons, including:

- Identifying attackers is difficult, as they may operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymizing procedures which make back-tracing difficult - and are often located in another jurisdiction. If they successfully breach security, they have also often gained enough administrative access to enable them to delete logs to cover their tracks.
- The sheer number of attempted attacks, often by automated vulnerability scanners and computer worms, is so large that organizations cannot spend time pursuing each.
- Law enforcement officers often lack the skills, interest or budget to pursue attackers. In addition, the identification of attackers across a network may require logs from various points in the network and in many countries, which may be difficult or time-consuming to obtain.

Where an attack succeeds and a breach occurs, many jurisdictions now have in place mandatory security breach notification laws.

Types of security and privacy

- Access control
- Anti-keyloggers
- Anti-malware
- Anti-spyware
- Anti-subversion software
- Anti-tamper software
- Anti-theft
- Antivirus software
- Cryptographic software
- Computer-aided dispatch (CAD)
- Firewall
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Log management software
- Parental control
- Records management
- Sandbox
- Security information management
- Security information and event management (SIEM)
- Software and operating system updating
- Vulnerability Management

Incident response planning

Incident response is an organized approach to addressing and managing the aftermath of a computer security incident or compromise with the goal of preventing a breach or thwarting a cyberattack. An incident that is not identified and managed at the time of intrusion typically escalates to a more damaging event such as a data breach or system failure. The intended outcome of a computer security incident response plan is to contain the incident, limit damage and assist recovery to business as usual. Responding to compromises quickly can mitigate exploited vulnerabilities, restore services and processes and minimize

losses.[155] Incident response planning allows an organization to establish a series of best practices to stop an intrusion before it causes damage. Typical incident response plans contain a set of written instructions that outline the organization's response to a cyberattack. Without a documented plan in place, an organization may not successfully detect an intrusion or compromise and stakeholders may not understand their roles, processes and procedures during an escalation, slowing the organization's response and resolution.

There are four key components of a computer security incident response plan:

1. Preparation: Preparing stakeholders on the procedures for handling computer security incidents or compromises
2. Detection and analysis: Identifying and investigating suspicious activity to confirm a security incident, prioritizing the response based on impact and coordinating notification of the incident
3. Containment, eradication and recovery: Isolating affected systems to prevent escalation and limit impact, pinpointing the genesis of the incident, removing malware, affected systems and bad actors from the environment and restoring systems and data when a threat no longer remains
4. Post incident activity: Post mortem analysis of the incident, its root cause and the organization's response with the intent of improving the incident response plan and future response efforts.[156]

Notable attacks and breaches

Some illustrative examples of different types of computer security breaches are given below.

Robert Morris and the first computer worm

In 1988, 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On 2 November 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers – the first internet "computer worm".[157] The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris who said "he wanted to count how many machines were connected to the Internet".[157]

Rome Laboratory

In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using trojan horses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of National Aeronautics and Space Administration's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.[158]

TJX customer credit card details

In early 2007, American apparel and home goods company TJX announced that it was the victim of an unauthorized computer systems intrusion[159] and that the hackers had accessed a system that stored data on credit card, debit card, check, and merchandise return transactions.[160]

Stuxnet attack

In 2010, the computer worm known as Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.[161] It did so by disrupting industrial programmable logic controllers (PLCs) in a targeted attack. This is generally believed to have been launched by Israel and the United States to disrupt Iran's nuclear program[162][163][164][165] – although neither has publicly admitted this.

Global surveillance disclosures

In early 2013, documents provided by Edward Snowden were published by *The Washington Post* and *The Guardian*[166][167] exposing the massive scale of NSA global surveillance. There were also indications that the NSA may have inserted a backdoor in a NIST standard for encryption.[168] This standard was later withdrawn due to widespread criticism.[169] The NSA additionally were revealed to have tapped the links between Google's data centers.[170]

Target and Home Depot breaches

A Ukrainian hacker known as Rescator broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards,[171] and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers.[172] Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee – meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Office of Personnel Management data breach

In April 2015, the Office of Personnel Management discovered it had been hacked more than a year earlier in a data breach, resulting in the theft of approximately 21.5 million personnel records handled by the office.[173] The Office of Personnel Management hack has been described by federal officials as among the largest breaches of government data in the history of the United States.[174] Data targeted in the breach included personally identifiable information such as Social Security numbers, names, dates and places of birth, addresses, and fingerprints of current and former government employees as well as anyone who had undergone a government background check.[175][176] It is believed the hack was perpetrated by Chinese hackers.[177]

Ashley Madison breach

In July 2015, a hacker group is known as "The Impact Team" successfully breached the extramarital relationship website Ashley Madison, created by Avid Life Media. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken

down permanently."[178] When Avid Life Media did not take the site offline the group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned; but the website remained to function.

Colonial Pipeline ransomware attack

In June 2021, the cyber attack took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast.[179]

Legal issues and global regulation

International legal issues of cyber attacks are complicated in nature. There is no global base of common rules to judge, and eventually punish, cybercrimes and cybercriminals - and where security firms or agencies do locate the cybercriminal behind the creation of a particular piece of malware or form of cyber attack, often the local authorities cannot take action due to lack of laws under which to prosecute.[180][181] Proving attribution for cybercrimes and cyberattacks is also a major problem for all law enforcement agencies. "Computer viruses switch from one country to another, from one jurisdiction to another – moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world."[180] The use of techniques such as dynamic DNS, fast flux and bullet proof servers add to the difficulty of investigation and enforcement.

Role of government

The role of the government is to make regulations to force companies and organizations to protect their systems, infrastructure and information from any cyberattacks, but also to protect its own national infrastructure such as the national power-grid.[182]

The government's regulatory role in cyberspace is complicated. For some, cyberspace was seen as a virtual space that was to remain free of government intervention, as can be seen in many of today's libertarian blockchain and bitcoin discussions.[183]

Many government officials and experts think that the government should do more and that there is a crucial need for improved regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem. R. Clarke said during a panel discussion at the RSA Security Conference in San Francisco, he believes that the "industry only responds when you threaten regulation. If the industry doesn't respond (to the threat), you have to follow through."[184] On the other hand, executives from the private sector agree that improvements are necessary, but think that government intervention would affect their ability to innovate efficiently. Daniel R. McCarthy analyzed this public-private partnership in cybersecurity and reflected on the role of cybersecurity in the broader constitution of political order.[185]

On 22 May 2020, the UN Security Council held its second ever informal meeting on cybersecurity to focus on cyber challenges to international peace. According to UN Secretary-General António Guterres, new technologies are too often used to violate rights.[186]

International actions

Many different teams and organizations exist, including:

- The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs.[187] The US-CERT, AT&T, Apple, Cisco, McAfee, Microsoft are all members of this international team.[188]
- The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime.[189]
- The purpose of the Messaging Anti-Abuse Working Group (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations.[190] France Telecom, Facebook, AT&T, Apple, Cisco, Sprint are some of the members of the MAAWG.[191]
- ENISA : The European Network and Information Security Agency (ENISA) is an agency of the European Union with the objective to improve network and information security in the European Union.

Europe

On 14 April 2016, the European Parliament and Council of the European Union adopted The General Data Protection Regulation (GDPR) (EU) 2016/679. GDPR, which became enforceable beginning 25 May 2018, provides for data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). GDPR requires that business processes that handle personal data be built with data protection by design and by default. GDPR also requires that certain organizations appoint a Data Protection Officer (DPO).

National actions

Computer emergency response teams

Most countries have their own computer emergency response team to protect network security.

Canada

Since 2010, Canada has had a cybersecurity strategy.[192][193] This functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.[194] The strategy has three main pillars: securing government systems, securing vital private cyber systems, and helping Canadians to be secure online.[193][194] There is also a Cyber Incident Management Framework to provide a coordinated response in the event of a cyber incident.[195][196]

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. It provides support to mitigate cyber threats, technical support to respond & recover from targeted cyber attacks, and provides online tools for members of Canada's critical infrastructure sectors.[197] It posts regular cybersecurity bulletins[198] & operates an online reporting tool where individuals and organizations can report a cyber incident.[199]

To inform the general public on how to protect themselves online, Public Safety Canada has partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations,[200] and launched the Cyber Security Cooperation Program.[201][202] They also run the GetCyberSafe portal for Canadian citizens, and Cyber Security Awareness Month during October.[203]

Public Safety Canada aims to begin an evaluation of Canada's cybersecurity strategy in early 2015.[194]

China

China's Central Leading Group for Internet Security and Informatization (Chinese: 中央网络安全和信息化领导小组) was established on 27 February 2014. This Leading Small Group (LSG) of the Chinese Communist Party is headed by General Secretary Xi Jinping himself and is staffed with relevant Party and state decision-makers. The LSG was created to overcome the incoherent policies and overlapping responsibilities that characterized China's former cyberspace decision-making mechanisms. The LSG oversees policy-making in the economic, political, cultural, social and military fields as they relate to network security and IT strategy. This LSG also coordinates major policy initiatives in the international arena that promote norms and standards favored by the Chinese government and that emphasizes the principle of national sovereignty in cyberspace.[204]

Germany

Berlin starts National Cyber Defense Initiative: On 16 June 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmdienst and other national organizations in Germany taking care of national security aspects. According to the Minister, the primary task of the new organization founded on 23 February 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet. Germany has also established the largest research institution for IT security in Europe, the Center for Research in Security and Privacy (CRISP) in Darmstadt.

India

Some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000.[205]

The National Cyber Security Policy 2013 is a policy framework by the Ministry of Electronics and Information Technology (MeitY) which aims to protect the public and private infrastructure from cyberattacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". CERT- In is the nodal agency which monitors the cyber threats in the country. The post of National Cyber Security Coordinator has also been created in the Prime Minister's Office (PMO).

The Indian Companies Act 2013 has also introduced cyber law and cybersecurity obligations on the part of Indian directors. Some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000 Update in 2013.[206]

South Korea

Following cyberattacks in the first half of 2013, when the government, news media, television stations, and bank websites were compromised, the national government committed to the training of 5,000 new cybersecurity experts by 2017. The South Korean government blamed its northern counterpart for these

attacks, as well as incidents that occurred in 2009, 2011,[207] and 2012, but Pyongyang denies the accusations.[208]

United States

Legislation

The 1986 18 U.S.C. § 1030 (https://www.law.cornell.edu/uscode/text/18/1030), the Computer Fraud and Abuse Act is the key legislation. It prohibits unauthorized access or damage of "protected computers" as defined in 18 U.S.C. § 1030(e)(2) (https://www.law.cornell.edu/uscode/text/18/1030#e_2). Although various other measures have been proposed[209][210] – none has succeeded.

In 2013, executive order 13636 *Improving Critical Infrastructure Cybersecurity* was signed, which prompted the creation of the NIST Cybersecurity Framework.

In response to the Colonial Pipeline ransomware attack[211] President Joe Biden signed Executive Order 14028[212] on May 12, 2021, to increase software security standards for sales to the government, tighten detection and security on existing systems, improve information sharing and training, establish a Cyber Safety Review Board, and improve incident response.

Standardized government testing services

The General Services Administration (GSA) has standardized the "penetration test" service as a pre-vetted support service, to rapidly address potential vulnerabilities, and stop adversaries before they impact US federal, state and local governments. These services are commonly referred to as Highly Adaptive Cybersecurity Services (HACS).

Agencies

The Department of Homeland Security has a dedicated division responsible for the response system, risk management program and requirements for cybersecurity in the United States called the National Cyber Security Division.[213][214] The division is home to US-CERT operations and the National Cyber Alert System.[214] The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure.[215]

The third priority of the FBI is to: "Protect the United States against cyber-based attacks and high-technology crimes",[216] and they, along with the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA) are part of the multi-agency task force, The Internet Crime Complaint Center, also known as IC3.[217]

In addition to its own specific duties, the FBI participates alongside non-profit organizations such as InfraGard.[218][219]

The Computer Crime and Intellectual Property Section (CCIPS) operates in the United States Department of Justice Criminal Division. The CCIPS is in charge of investigating computer crime and intellectual property crime and is specialized in the search and seizure of digital evidence in computers and networks.[220] In 2017, CCIPS published A Framework for a Vulnerability Disclosure Program for Online Systems to help organizations "clearly describe authorized vulnerability disclosure and discovery conduct, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law under the Computer Fraud and Abuse Act (18 U.S.C. § 1030)."[221]

The United States Cyber Command, also known as USCYBERCOM, "has the mission to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners."[222] It has no role in the protection of civilian networks.[223][224]

The U.S. Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during disasters, to aid in swift recovery after, and to ensure that first responders have access to effective communications services.[225]

The Food and Drug Administration has issued guidance for medical devices,[226] and the National Highway Traffic Safety Administration[227] is concerned with automotive cybersecurity. After being criticized by the Government Accountability Office,[228] and following successful attacks on airports and claimed attacks on airplanes, the Federal Aviation Administration has devoted funding to securing systems on board the planes of private manufacturers, and the Aircraft Communications Addressing and Reporting System.[229] Concerns have also been raised about the future Next Generation Air Transportation System.[230]

Computer emergency readiness team

"Computer emergency response team" is a name given to expert groups that handle computer security incidents. In the US, two distinct organizations exist, although they do work closely together.

- US-CERT: part of the National Cyber Security Division of the United States Department of Homeland Security.[231]
- CERT/CC: created by the Defense Advanced Research Projects Agency (DARPA) and run by the Software Engineering Institute (SEI).

Modern warfare

There is growing concern that cyberspace will become the next theater of warfare. As Mark Clayton from *The Christian Science Monitor* wrote in a 2015 article titled "The New Cyber Arms Race":

> In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships.[232]

This has led to new terms such as *cyberwarfare* and *cyberterrorism*. The United States Cyber Command was created in 2009[233] and many other countries have similar forces.

There are a few critical voices that question whether cybersecurity is as significant a threat as it is made out to be.[234][235][236]

Careers

Cybersecurity is a fast-growing field of IT concerned with reducing organizations' risk of hack or data breaches.[237] According to research from the Enterprise Strategy Group, 46% of organizations say that they have a "problematic shortage" of cybersecurity skills in 2016, up from 28% in 2015.[238] Commercial, government and non-governmental organizations all employ cybersecurity professionals. The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as finance, health care, and retail.[239] However, the use of the term "cybersecurity" is more prevalent in government job descriptions.[240]

Typical cybersecurity job titles and descriptions include:[241]

Security analyst

> Analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates using available tools and countermeasures to remedy the detected vulnerabilities and recommends solutions and best practices. Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures. May assist in the creation, implementation, or management of security solutions.

Security engineer

> Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mount the incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. May also review code or perform other security engineering methodologies.

Security architect

> Designs a security system or major components of a security system, and may head a security design team building a new security system.[242]

Security administrator

> Installs and manages organization-wide security systems. This position may also include taking on some of the tasks of a security analyst in smaller organizations.[243]

Chief Information Security Officer (CISO)

> A high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.[244]

Chief Security Officer (CSO)

> A high-level management position responsible for the entire security division/staff. A newer position is now deemed needed as security risks grow.

Data Protection Officer (DPO)

> A DPO is tasked with monitoring compliance with the UK GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.[245][246]

Security Consultant/Specialist/Intelligence

> Broad titles that encompass any one or all of the other roles or titles tasked with protecting computers, networks, software, data or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever-increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Student programs are also available for people interested in beginning a career in cybersecurity.[247][248] Meanwhile, a flexible and effective option for information security professionals of all experience levels to keep studying is online security training, including webcasts.[249][250] A wide range of certified courses are also available.[251]

In the United Kingdom, a nationwide set of cybersecurity forums, known as the U.K Cyber Security Forum, were established supported by the Government's cybersecurity strategy[252] in order to encourage start-ups and innovation and to address the skills gap[253] identified by the U.K Government.

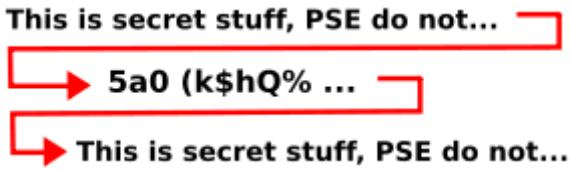
In Singapore, the Cyber Security Agency has issued a Singapore Operational Technology (OT) Cybersecurity Competency Framework (OTCCF). The framework defines emerging cybersecurity roles in Operational Technology. The OTCCF was endorsed by the Infocomm Media Development Authority (IMDA). It outlines the different OT cybersecurity job positions as well as the technical skills and core competencies necessary. It also depicts the many career paths available, including vertical and lateral advancement opportunities.[254]

Terminology

The following terms used with regards to computer security are explained below:

- Access authorization restricts access to a computer to a group of users through the use of authentication systems. These systems can protect either the whole computer, such as through an interactive login screen, or individual services, such as a FTP server. There are many methods for identifying and authenticating users, such as passwords, identification cards, smart cards, and biometric systems.
- Anti-virus software consists of computer programs that attempt to identify, thwart, and eliminate computer viruses and other malicious software (malware).
- Applications are executable code, so general practice is to disallow users the power to install them; to install only those which are known to be reputable – and to reduce the attack surface by installing as few as possible. They are typically run with least privilege, with a robust process in place to identify, test and install any released security patches or updates for them.
- Authentication techniques can be used to ensure that communication end-points are who they say they are.
- Automated theorem proving and other verification tools can be used to enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.

- Backups are one or more copies kept of important computer files. Typically, multiple copies will be kept at different locations so that if a copy is stolen or damaged, other copies will still exist.
- Capability and access control list techniques can be used to ensure privilege separation and mandatory access control. Capabilities vs. ACLs discusses their use.
- Chain of trust techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.
- Confidentiality is the nondisclosure of information except to another authorized person.[255]
- Cryptographic techniques can be used to defend data in transit between systems, reducing the probability that the data exchange between systems can be intercepted or modified.
- Cyberwarfare is an Internet-based conflict that involves politically motivated attacks on information and information systems. Such attacks can, for example, disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems.
- Data integrity is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.[256]
- Encryption is used to protect the confidentiality of a message. Cryptographically secure ciphers are designed to make any practical attempt of breaking them infeasible. Symmetric-key ciphers are suitable for bulk encryption using shared keys, and public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.



Cryptographic techniques involve transforming information, scrambling it, so it becomes unreadable during transmission. The intended recipient can unscramble the message; ideally, eavesdroppers cannot.

- Endpoint security software aids networks in preventing malware infection and data theft at network entry points made vulnerable by the prevalence of potentially infected devices such as laptops, mobile devices, and USB drives.[257]
- Firewalls serve as a gatekeeper system between networks, allowing only traffic that matches defined rules. They often include detailed logging, and may include intrusion detection and intrusion prevention features. They are near-universal between company local area networks and the Internet, but can also be used internally to impose traffic rules between networks if network segmentation is configured.
- A hacker is someone who seeks to breach defenses and exploit weaknesses in a computer system or network.
- Honey pots are computers that are intentionally left vulnerable to attack by crackers. They can be used to catch crackers and to identify their techniques.
- Intrusion-detection systems are devices or software applications that monitor networks or systems for malicious activity or policy violations.
- A microkernel is an approach to operating system design which has only the near-minimum amount of code running at the most privileged level – and runs other elements of the operating system such as device drivers, protocol stacks and file systems, in the safer, less privileged user space.
- Pinging. The standard "ping" application can be used to test if an IP address is in use. If it is, attackers may then try a port scan to detect which services are exposed.
- A port scan is used to probe an IP address for open ports to identify accessible network services and applications.

- A key logger is spyware which silently captures and stores each keystroke that a user types on the computer's keyboard.
- Social engineering is the use of deception to manipulate individuals to breach security.
- Logic bombs is a type of malware added to a legitimate program that lies dormant until it is triggered by a specific event.
- Zero trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.

Notable scholars

- Ross J. Anderson
- Annie Anton
- Adam Back
- Daniel J. Bernstein
- Matt Blaze
- Stefan Brands
- L. Jean Camp
- Lorrie Cranor
- Dorothy E. Denning
- Peter J. Denning
- Cynthia Dwork
- Chuck Easttom
- Deborah Estrin
- Joan Feigenbaum
- Ian Goldberg
- Shafi Goldwasser
- Lawrence A. Gordon
- Peter Gutmann
- Paul Kocher
- Monica S. Lam
- Butler Lampson
- Brian LaMacchia
- Susan Landau
- Carl Landwehr
- Kevin Mitnick
- Peter G. Neumann
- Susan Nycum
- Paul C. van Oorschot
- Roger R. Schell
- Bruce Schneier
- Dawn Song
- Gene Spafford
- Salvatore J. Stolfo
- Willis Ware
- Moti Yung

See also

- Attack tree
- Bicycle attack
- CAPTCHA
- Cloud computing security
- Comparison of antivirus software
- Content Disarm & Reconstruction
- Content Security Policy
- Countermeasure (computer)
- Cyber insurance
- Cyber self-defense
- Cyberbiosecurity
- Cybersecurity information technology list
- Dancing pigs
- Data security
- Defense strategy (computing)

- Fault tolerance
- Hardware security
- Human–computer interaction (security)
- Identity management
- Identity-based security
- Information security awareness
- Internet privacy
- Internet safety
- Internet security
- IT risk
- IT security standards
- Kill chain
- List of computer security certifications
- List of cyber warfare forces
- Open security
- Outline of computer security
- OWASP
- Physical information security
- Privacy software
- Separation of protection and security
- Software-defined perimeter

References

1. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security" (https://commons.erau.edu/jdfsl/vol12/iss2/8/). *Journal of Digital Forensics, Security and Law*. **12** (2). ISSN 1558-7215 (https://www.worldcat.org/issn/1558-7215).
2. "computer security | Definition & Facts | Britannica" (https://www.britannica.com/technology/computer-security). *www.britannica.com*. Retrieved 12 July 2022.
3. "Reliance spells end of road for ICT amateurs" (https://www.theaustralian.com.au/technology/opinion/reliance-spells-end-of-road-for-ict-amateurs/story-e6frgb0o-1226636267865). *The Australian*. 7 May 2013.
4. Kianpour, Mazaher; Kowalski, Stewart; Øverby, Harald (2021). "Systematically Understanding Cybersecurity Economics: A Survey" (https://doi.org/10.3390%2Fsu132413677). *Sustainability*. **13** (24): 13677. doi:10.3390/su132413677 (https://doi.org/10.3390%2Fsu132413677).
5. Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (https://kclpure.kcl.ac.uk/portal/files/97261726/PaG_6_2_Global_Cybersecurity_New_Directions_in_Theory_and_Methods.pdf) (PDF). *Politics and Governance*. **6** (2): 1–4. doi:10.17645/pag.v6i2.1569 (https://doi.org/10.17645%2Fpag.v6i2.1569).
6. Misa, Thomas J. (2016). "Computer Security Discourse at RAND, SDC, and NSA (1958-1970)" (https://dl.acm.org/doi/10.1109/MAHC.2016.48). *IEEE Annals of the History of Computing*. **38** (4): 12–25. doi:10.1109/MAHC.2016.48 (https://doi.org/10.1109%2FMAHC.2016.48). S2CID 17609542 (https://api.semanticscholar.org/CorpusID:17609542).

7. A. J. Neumann, N. Statland and R. D. Webb (1977). "Post-processing audit tools and techniques" (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf) (PDF). *nist.gov*. US Department of Commerce, National Bureau of Standards. pp. 11-3–11-4. Retrieved 19 June 2020.
8. Irwin, Luke (5 April 2018). "How NIST can protect the CIA triad, including the often overlooked 'I' – integrity" (https://blog.itgovernanceusa.com/blog/how-nist-can-protect-the-cia-triad-including-the-often-overlooked-i-integrity). *www.itgovernanceusa.com*. Retrieved 16 January 2021.
9. Perrin, Chad (30 June 2008). "The CIA Triad" (https://www.techrepublic.com/blog/security/the-cia-triad/488). *techrepublic.com*. Retrieved 31 May 2012.
10. Stoneburner, G.; Hayden, C.; Feringa, A. (2004). "Engineering Principles for Information Technology Security" (http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf) (PDF). csrc.nist.gov. doi:10.6028/NIST.SP.800-27rA (https://doi.org/10.6028%2FNIST.SP.800-27rA).
11. Yost, Jeffrey R. (April 2015). "The Origin and Early History of the Computer Security Software Products Industry" (https://ieeexplore.ieee.org/document/7116464). *IEEE Annals of the History of Computing*. **37** (2): 46–58. doi:10.1109/MAHC.2015.21 (https://doi.org/10.1109%2FMAHC.2015.21). ISSN 1934-1547 (https://www.worldcat.org/issn/1934-1547). S2CID 18929482 (https://api.semanticscholar.org/CorpusID:18929482).
12. Nakashima, Ellen (26 January 2008). "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions" (https://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261_pf.html). *The Washington Post*. Retrieved 8 February 2021.
13. Nicole Perlroth (7 February 2021). "How the U.S. Lost to Hackers" (https://ghostarchive.org/archive/20211228/https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html). *The New York Times*. Archived from the original (https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html) on 28 December 2021. Retrieved 9 February 2021.
14. "Computer Security and Mobile Security Challenges" (https://www.researchgate.net/publication/298807979). *researchgate.net*. 3 December 2015. Archived (https://web.archive.org/web/20161012010519/https://www.researchgate.net/publication/298807979_Computer_Security_and_Mobile_Security_Challenges) from the original on 12 October 2016. Retrieved 4 August 2016.
15. "Ghidra" (https://web.archive.org/web/20200815201448/https://www.nsa.gov/resources/everyone/ghidra/). Archived from the original (https://www.nsa.gov/resources/everyone/ghidra/) on 15 August 2020. Retrieved 17 August 2020.
16. Larabel, Michael (28 December 2017). "Syzbot: Google Continuously Fuzzing The Linux Kernel" (https://www.phoronix.com/scan.php?page=news_item&px=Syzbot-Linux-Kernel-Fuzzing/). *www.phoronix.com/*. Retrieved 25 March 2021.
17. GOsafeonline (12 November 2014). "Distributed Denial of Service Attack" (https://www.csa.gov.sg/gosafeonline/go-safe-for-business/smes/distributed-denial-of-service-attack). *csa.gov.sg*. Archived (https://web.archive.org/web/20160806080013/https://www.csa.gov.sg/gosafeonline/go-safe-for-business/smes/distributed-denial-of-service-attack) from the original on 6 August 2016. Retrieved 12 November 2014.
18. Webroot (24 July 2018). "Multi-Vector Attacks Demand Multi-Vector Protection" (https://www.msspalert.com/cybersecurity-guests/multi-vector-attacks-demand-multi-vector-protection/). *MSSP Alert*. Retrieved 11 May 2022.
19. Millman, Renee (15 December 2017). "New polymorphic malware evades three-quarters of AV scanners" (https://www.scmagazineuk.com/new-polymorphic-malware-evades-three-quarters-of-av-scanners/article/718757/). *SC Magazine UK*.

20. "Identifying Phishing Attempts" (https://web.archive.org/web/20150913200707/http://www.case.edu/its/kba/its-kba-27196-phishing-attempt/). Case. Archived from the original (https://www.case.edu/its/kba/its-kba-27196-phishing-attempt/) on 13 September 2015. Retrieved 4 July 2016.
21. Lazarus, Ari (23 February 2018). "Phishers send fake invoices" (https://www.consumer.ftc.gov/blog/2018/02/phishers-send-fake-invoices). *Consumer Information*. Retrieved 17 February 2020.
22. Eilam, Eldad (2005). *Reversing: secrets of reverseengineering*. John Wiley & Sons. ISBN 978-0-7645-7481-8.
23. Arcos Sergio. "Social Engineering" (http://upcommons.upc.edu/pfc/bitstream/2099.1/12289/1/73827.pdf) (PDF). *upc.edu*. Archived (https://web.archive.org/web/20131203043630/http://upcommons.upc.edu/pfc/bitstream/2099.1/12289/1/73827.pdf) (PDF) from the original on 3 December 2013. Retrieved 16 April 2019.
24. Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn" (https://www.ft.com/intl/cms/s/0/83b4e9be-db16-11e5-a72f-1e7744c66818.html#axzz41pN5YBV4). *Financial Times*. No. 25 February 2016. Archived (https://web.archive.org/web/20160623105523/http://www.ft.com/intl/cms/s/0/83b4e9be-db16-11e5-a72f-1e7744c66818.html#axzz41pN5YBV4) from the original on 23 June 2016. Retrieved 7 May 2016.
25. "Bucks leak tax info of players, employees as result of email scam" (http://espn.go.com/nba/story/_/id/15615363/milwaukee-bucks-leak-tax-information-players-employees-result-email-scam). Associated Press. 20 May 2016. Archived (https://web.archive.org/web/20160520144908/http://espn.go.com/nba/story/_/id/15615363/milwaukee-bucks-leak-tax-informatiopn-players-employees-result-email-scam) from the original on 20 May 2016. Retrieved 20 May 2016.
26. "What is Spoofing? – Definition from Techopedia" (https://www.techopedia.com/definition/5398/spoofing). *techopedia.com*. Archived (https://web.archive.org/web/20160630134737/https://www.techopedia.com/definition/5398/spoofing) from the original on 30 June 2016. Retrieved 16 January 2022.
27. Butterfield, Andrew; Ngondi, Gerard Ekembe, eds. (21 January 2016). *spoofing* (http://www.oxfordreference.com/view/10.1093/acref/9780199688975.001.0001/acref-9780199688975-e-4987). *Oxford Reference*. Oxford University Press. doi:10.1093/acref/9780199688975.001.0001 (https://doi.org/10.1093%2Facref%2F9780199688975.001.0001). ISBN 9780199688975. Retrieved 8 October 2017.
28. Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*. Advances in Computer Vision and Pattern Recognition. London: Springer. doi:10.1007/978-1-4471-6524-8 (https://doi.org/10.1007%2F978-1-4471-6524-8). ISBN 978-1-4471-6524-8. ISSN 2191-6594 (https://www.worldcat.org/issn/2191-6594). LCCN 2014942635 (https://lccn.loc.gov/2014942635). S2CID 27594864 (https://api.semanticscholar.org/CorpusID:27594864).
29. Gallagher, Sean (14 May 2014). "Photos of an NSA "upgrade" factory show Cisco router getting implant" (https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/). *Ars Technica*. Archived (https://web.archive.org/web/20140804130416/http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/) from the original on 4 August 2014. Retrieved 3 August 2014.
30. Bendovschi, Andreea (2015). "Cyber-Attacks – Trends, Patterns and Security Countermeasures" (https://doi.org/10.1016%2FS2212-5671%2815%2901077-1). *Procedia Economics and Finance*. **28**: 24–31. doi:10.1016/S2212-5671(15)01077-1 (https://doi.org/10.1016%2FS2212-5671%2815%2901077-1).
31. Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.

32. K. Reimers, D. Andersson (2017) POST-SECONDARY EDUCATION NETWORK SECURITY: THE END USER CHALLENGE AND EVOLVING THREATS (https://library.iated.org/view/REIMERS2017POS), ICERI2017 Proceedings, pp. 1787-1796.
33. "Verizon Data Breach Investigations Report 2020" (https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf) (PDF). *verizon.com*. Retrieved 17 September 2021.
34. Schlienger, Thomas; Teufel, Stephanie (2003). "Information security culture-from analysis to change". *South African Computer Journal*. **31**: 46–52.
35. Lin, Tom C. W. (3 July 2017). "The New Market Manipulation". *Emory Law Journal*. **66**: 1253. SSRN 2996896 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2996896).
36. Lin, Tom C. W. (2016). "Financial Weapons of War". *Minnesota Law Review*. SSRN 2765010 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765010).
37. Pagliery, Jose (18 November 2014). "Hackers attacked the U.S. energy grid 79 times this year" (https://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/). *CNN Money*. Cable News Network. Archived (https://web.archive.org/web/20150218070238/https://money.cnn.com/2014/11/18/technology/security/energy-grid-hack) from the original on 18 February 2015. Retrieved 16 April 2015.
38. P. G. Neumann, "Computer Security in Aviation," presented at International Conference on Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security, 1997.
39. J. Zellan, Aviation Security. Hauppauge, NY: Nova Science, 2003, pp. 65–70.
40. "Air Traffic Control Systems Vulnerabilities Could Make for Unfriendly Skies [Black Hat] - SecurityWeek.Com" (http://www.securityweek.com/air-traffic-control-systems-vulnerabilities-could-make-unfriendly-skies-black-hat). Archived (https://web.archive.org/web/20150208070914/http://www.securityweek.com/air-traffic-control-systems-vulnerabilities-could-make-unfriendly-skies-black-hat) from the original on 8 February 2015.
41. "Hacker Says He Can Break into Airplane Systems Using In-Flight Wi-Fi" (https://www.npr.org/blogs/alltechconsidered/2014/08/04/337794061/hacker-says-he-can-break-into-airplane-systems-using-in-flight-wi-fi). *NPR*. 4 August 2014. Archived (https://web.archive.org/web/20150208072554/http://www.npr.org/blogs/alltechconsidered/2014/08/04/337794061/hacker-says-he-can-break-into-airplane-systems-using-in-flight-wi-fi) from the original on 8 February 2015. Retrieved 19 March 2020.
42. Jim Finkle (4 August 2014). "Hacker says to show passenger jets at risk of cyber attack" (https://www.reuters.com/article/us-cybersecurity-hackers-airplanes-idUSKBN0G40WQ20140804). *Reuters*. Archived (https://web.archive.org/web/20151013061705/http://www.reuters.com/article/2014/08/04/us-cybersecurity-hackers-airplanes-idUSKBN0G40WQ20140804) from the original on 13 October 2015. Retrieved 21 November 2021.
43. "Pan-European Network Services (PENS) - Eurocontrol.int" (https://www.eurocontrol.int/articles/pan-european-network-services-pens). Archived (https://web.archive.org/web/20161212175606/https://www.eurocontrol.int/articles/pan-european-network-services-pens) from the original on 12 December 2016.
44. "Centralised Services: NewPENS moves forward - Eurocontrol.int" (https://www.eurocontrol.int/news/centralised-services-newpens-moves-forward). 17 January 2016. Archived (https://web.archive.org/web/20170319025329/https://www.eurocontrol.int/news/centralised-services-newpens-moves-forward) from the original on 19 March 2017.
45. "NextGen Data Communication" (https://web.archive.org/web/20150313110025/http://www.faa.gov/nextgen/update/progress_and_plans/data_comm/). FAA. Archived from the original (https://www.faa.gov/nextgen/update/progress_and_plans/data_comm/) on 13 March 2015. Retrieved 15 June 2017.

46. "Is Your Watch Or Thermostat A Spy? Cybersecurity Firms Are On It" (https://www.npr.org/blogs/alltechconsidered/2014/08/06/338334508/is-your-watch-or-thermostat-a-spy-cyber-security-firms-are-on-it). *NPR*. 6 August 2014. Archived (https://web.archive.org/web/20150211064650/http://www.npr.org/blogs/alltechconsidered/2014/08/06/338334508/is-your-watch-or-thermostat-a-spy-cyber-security-firms-are-on-it) from the original on 11 February 2015.
47. Melvin Backman (18 September 2014). "Home Depot: 56 million cards exposed in breach" (https://money.cnn.com/2014/09/18/technology/security/home-depot-hack/). CNNMoney. Archived (https://web.archive.org/web/20141218221105/https://money.cnn.com/2014/09/18/technology/security/home-depot-hack/) from the original on 18 December 2014.
48. "Staples: Breach may have affected 1.16 million customers' cards" (http://fortune.com/2014/12/19/staples-cards-affected-breach/). *Fortune.com*. 19 December 2014. Archived (https://web.archive.org/web/20141221160612/http://fortune.com/2014/12/19/staples-cards-affected-breach/) from the original on 21 December 2014. Retrieved 21 December 2014.
49. "Target: 40 million credit cards compromised" (https://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html). *CNN*. 19 December 2013. Archived (https://web.archive.org/web/20171201035530/https://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html) from the original on 1 December 2017. Retrieved 29 November 2017.
50. Cowley, Stacy (2 October 2017). "2.5 Million More People Potentially Exposed in Equifax Breach" (https://www.nytimes.com/2017/10/02/business/equifax-breach.html). *The New York Times*. Archived (https://web.archive.org/web/20171201054900/https://www.nytimes.com/2017/10/02/business/equifax-breach.html) from the original on 1 December 2017. Retrieved 29 November 2017.
51. Jim Finkle (23 April 2014). "Exclusive: FBI warns healthcare sector vulnerable to cyber attacks" (https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423). *Reuters*. Archived (https://web.archive.org/web/20160604120725/http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423) from the original on 4 June 2016. Retrieved 23 May 2016.
52. Seals, Tara (6 November 2015). "Lack of Employee Security Training Plagues US Businesses" (https://www.infosecurity-magazine.com/news/lack-of-employee-security-training/). *Infosecurity Magazine*. Archived (https://web.archive.org/web/20171109081033/https://www.infosecurity-magazine.com/news/lack-of-employee-security-training/) from the original on 9 November 2017. Retrieved 8 November 2017.
53. Bright, Peter (15 February 2011). "Anonymous speaks: the inside story of the HBGary hack" (https://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/). Arstechnica.com. Archived (https://web.archive.org/web/20110327045801/http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars) from the original on 27 March 2011. Retrieved 29 March 2011.
54. Anderson, Nate (9 February 2011). "How one man tracked down Anonymous – and paid a heavy price" (https://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars/). Arstechnica.com. Archived (https://web.archive.org/web/20110329090824/http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars) from the original on 29 March 2011. Retrieved 29 March 2011.
55. Palilery, Jose (24 December 2014). "What caused Sony hack: What we know now" (https://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/). *CNN Money*. Archived (https://web.archive.org/web/20150104195455/https://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/) from the original on 4 January 2015. Retrieved 4 January 2015.

56. James Cook (16 December 2014). "Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far" (http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12). *Business Insider*. Archived (https://web.archive.org/web/20141217204735/http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12) from the original on 17 December 2014. Retrieved 18 December 2014.
57. Timothy B. Lee (18 January 2015). "The next frontier of hacking: your car" (https://www.vox.com/2015/1/18/7629603/car-hacking-dangers). *Vox*. Archived (https://web.archive.org/web/20170317212726/http://www.vox.com/2015/1/18/7629603/car-hacking-dangers) from the original on 17 March 2017.
58. Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf) (PDF) (Report). 6 February 2015. Archived (https://web.archive.org/web/20161109040112/http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf) (PDF) from the original on 9 November 2016. Retrieved 4 November 2016.
59. "Cybersecurity expert: It will take a 'major event' for companies to take this issue seriously" (https://www.aol.com/article/news/2016/12/26/expert-warns-major-event-will-need-to-happen-for-cybersecurity/21632630/). *AOL.com*. Archived (https://web.archive.org/web/20170120180918/https://www.aol.com/article/news/2016/12/26/expert-warns-major-event-will-need-to-happen-for-cybersecurity/21632630/) from the original on 20 January 2017. Retrieved 22 January 2017.
60. "The problem with self-driving cars: who controls the code?" (https://www.theguardian.com/technology/2015/dec/23/the-problem-with-self-driving-cars-who-controls-the-code). *The Guardian*. 23 December 2015. Archived (https://web.archive.org/web/20170316152605/https://www.theguardian.com/technology/2015/dec/23/the-problem-with-self-driving-cars-who-controls-the-code) from the original on 16 March 2017. Retrieved 22 January 2017.
61. Stephen Checkoway; Damon McCoy; Brian Kantor; Danny Anderson; Hovav Shacham; Stefan Savage; Karl Koscher; Alexei Czeskis; Franziska Roesner; Tadayoshi Kohno (2011). *Comprehensive Experimental Analyses of Automotive Attack Surfaces* (http://www.autosec.org/pubs/cars-usenixsec2011.pdf) (PDF). SEC'11 Proceedings of the 20th USENIX conference on Security. Berkeley, CA, US: USENIX Association. p. 6. Archived (https://web.archive.org/web/20150221064614/http://www.autosec.org/pubs/cars-usenixsec2011.pdf) (PDF) from the original on 21 February 2015.
62. Greenberg, Andy (21 July 2015). "Hackers Remotely Kill a Jeep on the Highway – With Me in It" (https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/). *Wired*. Archived (https://web.archive.org/web/20170119103855/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/) from the original on 19 January 2017. Retrieved 22 January 2017.
63. "Hackers take control of car, drive it into a ditch" (https://www.independent.co.uk/news/science/hackers-remotely-carjack-jeep-from-10-miles-away-and-drive-it-into-ditch-10406554.html). *The Independent*. 22 July 2015. Archived (https://web.archive.org/web/20170202061247/http://www.independent.co.uk/news/science/hackers-remotely-carjack-jeep-from-10-miles-away-and-drive-it-into-ditch-10406554.html) from the original on 2 February 2017. Retrieved 22 January 2017.
64. "Tesla fixes software bug that allowed Chinese hackers to control car remotely" (https://www.telegraph.co.uk/technology/2016/09/21/tesla-fixes-software-bug-that-allowed-chinese-hackers-to-control/). *The Telegraph*. 21 September 2016. Archived (https://web.archive.org/web/20170202014932/http://www.telegraph.co.uk/technology/2016/09/21/tesla-fixes-software-bug-that-allowed-chinese-hackers-to-control/) from the original on 2 February 2017. Retrieved 22 January 2017.

65. Kang, Cecilia (19 September 2016). "Self-Driving Cars Gain Powerful Ally: The Government" (https://www.nytimes.com/2016/09/20/technology/self-driving-cars-guidelines.html?_r=0). *The New York Times*. Archived (https://web.archive.org/web/20170214045032/https://www.nytimes.com/2016/09/20/technology/self-driving-cars-guidelines.html?_r=0) from the original on 14 February 2017. Retrieved 22 January 2017.
66. "Federal Automated Vehicles Policy" (https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf) (PDF). Archived (https://web.archive.org/web/20170121161404/https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf) (PDF) from the original on 21 January 2017. Retrieved 22 January 2017.
67. "Gary McKinnon profile: Autistic 'hacker' who started writing computer programs at 14" (https://www.telegraph.co.uk/news/worldnews/northamerica/usa/4320901/Gary-McKinnon-profile-Autistic-hacker-who-started-writing-computer-programs-at-14.html). *The Daily Telegraph*. London. 23 January 2009. Archived (https://web.archive.org/web/20100602065423/http://www.telegraph.co.uk/news/worldnews/northamerica/usa/4320901/Gary-McKinnon-profile-Autistic-hacker-who-started-writing-computer-programs-at-14.html) from the original on 2 June 2010.
68. "Gary McKinnon extradition ruling due by 16 October" (https://www.bbc.co.uk/news/uk-19506090). *BBC News*. 6 September 2012. Archived (https://web.archive.org/web/20120906185731/http://www.bbc.co.uk/news/uk-19506090) from the original on 6 September 2012. Retrieved 25 September 2012.
69. Law Lords Department (30 July 2008). "House of Lords – Mckinnon V Government of The United States of America and Another" (https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm). Publications.parliament.uk. Archived (https://web.archive.org/web/20090307045833/http://www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm) from the original on 7 March 2009. Retrieved 30 January 2010. "15. … alleged to total over $700,000"
70. "NSA Accessed Mexican President's Email" (http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html) Archived (https://web.archive.org/web/20151106193613/http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html) 6 November 2015 at the Wayback Machine, 20 October 2013, Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, spiegel.de
71. Sanders, Sam (4 June 2015). "Massive Data Breach Puts 4 Million Federal Employees' Records at Risk" (https://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk). *NPR*. Archived (https://web.archive.org/web/20150605041629/http://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk) from the original on 5 June 2015. Retrieved 5 June 2015.
72. Liptak, Kevin (4 June 2015). "U.S. government hacked; feds think China is the culprit" (http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/). *CNN*. Archived (https://web.archive.org/web/20150606063139/http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/) from the original on 6 June 2015. Retrieved 5 June 2015.
73. Sean Gallagher. "Encryption "would not have helped" at OPM, says DHS official" (https://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/). Archived (https://web.archive.org/web/20170624014751/https://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/) from the original on 24 June 2017.

74. Davis, Michelle R. (19 October 2015). "Schools Learn Lessons From Security Breaches" (http://www.edweek.org/ew/articles/2015/10/21/lessons-learned-from-security-breaches.html). *Education Week*. Archived (https://web.archive.org/web/20160610130749/http://www.edweek.org/ew/articles/2015/10/21/lessons-learned-from-security-breaches.html) from the original on 10 June 2016. Retrieved 23 May 2016.
75. "Internet of Things Global Standards Initiative" (http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx). *ITU*. Archived (https://web.archive.org/web/20150626125229/http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx) from the original on 26 June 2015. Retrieved 26 June 2015.
76. Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; Ko, Hajoon; Eyers, David (2015). "Twenty Cloud Security Considerations for Supporting the Internet of Things" (https://www.repository.cam.ac.uk/handle/1810/250441). *IEEE Internet of Things Journal*. **3** (3): 269–284. doi:10.1109/JIOT.2015.2460333 (https://doi.org/10.1109%2FJIOT.2015.2460333). S2CID 4732406 (https://api.semanticscholar.org/CorpusID:4732406).
77. Chris Clearfield. "Why The FTC Can't Regulate The Internet Of Things" (https://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/). *Forbes*. Archived (https://web.archive.org/web/20150627090938/http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/) from the original on 27 June 2015. Retrieved 26 June 2015.
78. "Internet of Things: Science Fiction or Business Fact?" (https://hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf) (PDF). *Harvard Business Review*. Retrieved 4 November 2016.
79. Ovidiu Vermesan; Peter Friess. "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems" (http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf) (PDF). River Publishers. Archived (https://web.archive.org/web/20161012010519/http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf) (PDF) from the original on 12 October 2016. Retrieved 4 November 2016.
80. Christopher Clearfield "Rethinking Security for the Internet of Things" Harvard Business Review Blog, 26 June 2013 (http://blogs.hbr.org/2013/06/rethinking-security-for-the-in) Archived (https://web.archive.org/web/20130920145534/http://blogs.hbr.org/2013/06/rethinking-security-for-the-in/) 20 September 2013 at the Wayback Machine/
81. "Hotel room burglars exploit critical flaw in electronic door locks" (https://arstechnica.com/security/2012/11/hotel-room-burglars-exploit-critical-flaw-in-electronic-door-locks/). *Ars Technica*. 26 November 2012. Archived (https://web.archive.org/web/20160514002208/http://arstechnica.com/security/2012/11/hotel-room-burglars-exploit-critical-flaw-in-electronic-door-locks/) from the original on 14 May 2016. Retrieved 23 May 2016.
82. "Hospital Medical Devices Used As Weapons in Cyberattacks" (http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751). *Dark Reading*. 6 August 2015. Archived (https://web.archive.org/web/20160529002947/http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751) from the original on 29 May 2016. Retrieved 23 May 2016.
83. Jeremy Kirk (17 October 2012). "Pacemaker hack can deliver deadly 830-volt jolt" (http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html). *Computerworld*. Archived (https://web.archive.org/web/20160604201841/http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html) from the original on 4 June 2016. Retrieved 23 May 2016.

84. News, Kaiser Health (17 November 2014). "How Your Pacemaker Will Get Hacked" (http://www.thedailybeast.com/articles/2014/11/17/how-your-pacemaker-will-get-hacked.html). *The Daily Beast*. Archived (https://web.archive.org/web/20160520155616/http://www.thedailybeast.com/articles/2014/11/17/how-your-pacemaker-will-get-hacked.html) from the original on 20 May 2016. Retrieved 23 May 2016. {{cite news}}: |last1= has generic name (help)
85. Leetaru, Kalev. "Hacking Hospitals And Holding Hostages: Cybersecurity In 2016" (https://www.forbes.com/sites/kalevleetaru/2016/03/29/hacking-hospitals-and-holding-hostages-cybersecurity-in-2016/). *Forbes*. Archived (https://web.archive.org/web/20161229104021/http://www.forbes.com/sites/kalevleetaru/2016/03/29/hacking-hospitals-and-holding-hostages-cybersecurity-in-2016/) from the original on 29 December 2016. Retrieved 29 December 2016.
86. "Cyber-Angriffe: Krankenhäuser rücken ins Visier der Hacker" (http://www.wiwo.de/technologie/digitale-welt/cyber-angriffe-krankenhaeuser-ruecken-ins-visier-der-hacker/14946040.html). Wirtschafts Woche. Archived (https://web.archive.org/web/20161229101724/http://www.wiwo.de/technologie/digitale-welt/cyber-angriffe-krankenhaeuser-ruecken-ins-visier-der-hacker/14946040.html) from the original on 29 December 2016. Retrieved 29 December 2016.
87. "Hospitals keep getting attacked by ransomware – Here's why" (http://www.businessinsider.com/hospital-ransomware-hack-2016-5). *Business Insider*. Archived (https://web.archive.org/web/20161229101247/http://www.businessinsider.com/hospital-ransomware-hack-2016-5) from the original on 29 December 2016. Retrieved 29 December 2016.
88. "MedStar Hospitals Recovering After 'Ransomware' Hack" (https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121). *NBC News*. Archived (https://web.archive.org/web/20161229103355/https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121) from the original on 29 December 2016. Retrieved 29 December 2016.
89. Pauli, Darren. "US hospitals hacked with ancient exploits" (https://www.theregister.co.uk/2016/06/28/medjack/). *The Register*. Archived (https://web.archive.org/web/20161116141207/http://www.theregister.co.uk/2016/06/28/medjack) from the original on 16 November 2016. Retrieved 29 December 2016.
90. Pauli, Darren. "Zombie OS lurches through Royal Melbourne Hospital spreading virus" (https://www.theregister.co.uk/2016/01/19/melbourne_hospital_pathology_wing_splattered_by_virus/). *The Register*. Archived (https://web.archive.org/web/20161229101019/http://www.theregister.co.uk/2016/01/19/melbourne_hospital_pathology_wing_splattered_by_virus/) from the original on 29 December 2016. Retrieved 29 December 2016.
91. "Hacked Lincolnshire hospital computer systems 'back up' " (https://www.bbc.com/news/uk-england-humber-37849746). *BBC News*. 2 November 2016. Archived (https://web.archive.org/web/20161229101819/http://www.bbc.com/news/uk-england-humber-37849746) from the original on 29 December 2016. Retrieved 29 December 2016.
92. "Lincolnshire operations cancelled after network attack" (https://www.bbc.com/news/uk-england-humber-37822084). *BBC News*. 31 October 2016. Archived (https://web.archive.org/web/20161229101209/http://www.bbc.com/news/uk-england-humber-37822084) from the original on 29 December 2016. Retrieved 29 December 2016.
93. "Legion cyber-attack: Next dump is sansad.nic.in, say hackers" (http://indianexpress.com/article/technology/tech-news-technology/legion-hacking-no-political-agenda-just-computer-geeks-says-hacker-4423167/). *The Indian Express*. 12 December 2016. Archived (https://web.archive.org/web/20161229100631/http://indianexpress.com/article/technology/tech-news-technology/legion-hacking-no-political-agenda-just-computer-geeks-says-hacker-4423167/) from the original on 29 December 2016. Retrieved 29 December 2016.

94. "Former New Hampshire Psychiatric Hospital Patient Accused Of Data Breach" (http://boston.cbslocal.com/2016/12/27/former-patient-accused-data-breech-new-hampshire-psychiatric-hospital/). CBS Boston. 27 December 2016. Archived (https://web.archive.org/web/20170929233237/http://boston.cbslocal.com/2016/12/27/former-patient-accused-data-breech-new-hampshire-psychiatric-hospital/) from the original on 29 September 2017. Retrieved 29 December 2016.
95. "Texas Hospital hacked, affects nearly 30,000 patient records" (http://www.healthcareitnews.com/news/texas-hospital-hacked-affects-nearly-30000-patient-records). Healthcare IT News. 4 November 2016. Archived (https://web.archive.org/web/20161229171117/http://www.healthcareitnews.com/news/texas-hospital-hacked-affects-nearly-30000-patient-records) from the original on 29 December 2016. Retrieved 29 December 2016.
96. Becker, Rachel (27 December 2016). "New cybersecurity guidelines for medical devices tackle evolving threats" (https://www.theverge.com/2016/12/27/14095166/fda-guidance-medical-device-cybersecurity-cyberattack-hacking-guidelines). *The Verge*. Archived (https://web.archive.org/web/20161228210257/http://www.theverge.com/2016/12/27/14095166/fda-guidance-medical-device-cybersecurity-cyberattack-hacking-guidelines) from the original on 28 December 2016. Retrieved 29 December 2016.
97. "Postmarket Management of Cybersecurity in Medical Devices" (https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf) (PDF). *Food and Drug Administration*. 28 December 2016. Archived (https://web.archive.org/web/20161229102808/https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf) (PDF) from the original on 29 December 2016. Retrieved 29 December 2016.
98. Brandt, Jaclyn (18 June 2018). "D.C. distributed energy proposal draws concerns of increased cybersecurity risks" (https://dailyenergyinsider.com/featured/13110-d-c-distributed-energy-proposal-draws-concerns-of-increased-cybersecurity-risks/). *Daily Energy Insider*. Retrieved 4 July 2018.
99. Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. Congressional Research Service, Government, and Finance Division. Washington DC: The Library of Congress.
100. Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". *ACM Transactions on Information and System Security*. **5** (4): 438–457. doi:10.1145/581271.581274 (https://doi.org/10.1145%2F581271.581274). S2CID 1500788 (https://api.semanticscholar.org/CorpusID:1500788).
101. Han, Chen; Dongre, Rituja (2014). "Q&A. What Motivates Cyber-Attackers?" (https://timreview.ca/article/838). *Technology Innovation Management Review*. **4** (10): 40–42. doi:10.22215/timreview/838 (https://doi.org/10.22215%2Ftimreview%2F838). ISSN 1927-0321 (https://www.worldcat.org/issn/1927-0321).
102. Chermick, Steven; Freilich, Joshua; Holt, Thomas (April 2017). "Exploring the Subculture of Ideologically Motivated Cyber-Attackers". *Journal of Contemporary Criminal Justice*. **33** (3): 212–233. doi:10.1177/1043986217699100 (https://doi.org/10.1177%2F1043986217699100). S2CID 152277480 (https://api.semanticscholar.org/CorpusID:152277480).
103. Anderson, Ross (2020). *Security engineering : a guide to building dependable distributed systems* (Third ed.). Indianapolis, IN. ISBN 978-1-119-64281-7. OCLC 1224516855 (https://www.worldcat.org/oclc/1224516855).
104. RFC 2828 (https://datatracker.ietf.org/doc/html/rfc2828) Internet Security Glossary
105. CNSS Instruction No. 4009 (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) Archived (https://web.archive.org/web/20120227163121/http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) 27 February 2012 at the Wayback Machine dated 26 April 2010

106. "InfosecToday Glossary" (http://www.infosectoday.com/Articles/Glossary.pdf) (PDF). Archived (https://web.archive.org/web/20141120041536/http://www.infosectoday.com/Articles/Glossary.pdf) (PDF) from the original on 20 November 2014.
107. Definitions: IT Security Architecture (http://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture) Archived (https://web.archive.org/web/20140315012754/http://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture) 15 March 2014 at the Wayback Machine. SecurityArchitecture.org, Jan 2006
108. Jannsen, Cory. "Security Architecture" (http://www.techopedia.com/definition/72/security-architecture). *Techopedia*. Janalta Interactive Inc. Archived (https://web.archive.org/web/20141003064643/http://www.techopedia.com/definition/72/security-architecture) from the original on 3 October 2014. Retrieved 9 October 2014.
109. Woodie, Alex (9 May 2016). "Why ONI May Be Our Best Hope for Cyber Security Now" (http://www.datanami.com/2016/05/09/oni-may-best-hope-cyber-security-now/). Archived (https://web.archive.org/web/20160820015812/https://www.datanami.com/2016/05/09/oni-may-best-hope-cyber-security-now/) from the original on 20 August 2016. Retrieved 13 July 2016.
110. "Firms lose more to electronic than physical theft" (https://www.reuters.com/article/us-crime-fraud-idUSTRE69H25820101018). *Reuters*. 18 October 2010. Archived (https://web.archive.org/web/20150925113829/http://www.reuters.com/article/2010/10/18/us-crime-fraud-idUSTRE69H25820101018) from the original on 25 September 2015.
111. Walkowski, Debbie (9 July 2019). "What Is The CIA Triad?" (https://www.f5.com/labs/articles/education/what-is-the-cia-triad.html). *F5 Labs*. Retrieved 25 February 2020.
112. "Knowing Value of Data Assets is Crucial to Cybersecurity Risk Management | SecurityWeek.Com" (https://www.securityweek.com/knowing-value-data-assets-crucial-cybersecurity-risk-management). *www.securityweek.com*. Retrieved 25 February 2020.
113. Foreman, P: *Vulnerability Management*, page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5
114. Academy, Cisco Networking (17 June 2018). *CCNA Cybersecurity Operations Companion Guide* (https://books.google.com/books?id=FxRbDwAAQBAJ&q=Vulnerabilities+can+be+discovered+with+a+vulnerability+scanner,+which+analyzes+a+computer+system+in+search+of+known+vulnerabilities&pg=SA5-PA83). Cisco Press. ISBN 978-0-13-516624-6.
115. Alan Calder and Geraint Williams (2014). *PCI DSS: A Pocket Guide, 3rd Edition*. ISBN 978-1-84928-554-4. "network vulnerability scans at least quarterly and after any significant change in the network"
116. Harrison, J. (2003). "Formal verification at Intel". *18th Annual IEEE Symposium of Logic in Computer Science, 2003. Proceedings*. pp. 45–54. doi:10.1109/LICS.2003.1210044 (https://doi.org/10.1109%2FLICS.2003.1210044). ISBN 978-0-7695-1884-8. S2CID 44585546 (https://api.semanticscholar.org/CorpusID:44585546).
117. Umrigar, Zerksis D.; Pitchumani, Vijay (1983). "Formal verification of a real-time hardware design" (http://portal.acm.org/citation.cfm?id=800667). *Proceeding DAC '83 Proceedings of the 20th Design Automation Conference*. IEEE Press. pp. 221–7. ISBN 978-0-8186-0026-5.
118. "Abstract Formal Specification of the seL4/ARMv6 API" (https://web.archive.org/web/20150521171234/https://sel4.systems/Docs/seL4-spec.pdf) (PDF). Archived from the original (https://sel4.systems/Docs/seL4-spec.pdf) (PDF) on 21 May 2015. Retrieved 19 May 2015.
119. Christoph Baumann, Bernhard Beckert, Holger Blasum, and Thorsten Bormer Ingredients of Operating System Correctness? Lessons Learned in the Formal Verification of PikeOS (http://www-wjp.cs.uni-saarland.de/publikationen/Ba10EW.pdf) Archived (https://web.archive.org/web/20110719110932/http://www-wjp.cs.uni-saarland.de/publikationen/Ba10EW.pdf) 19 July 2011 at the Wayback Machine

120. "Getting it Right" (http://www.ganssle.com/rants/gettingitright.htm) Archived (https://web.archive.org/web/20130504191958/http://www.ganssle.com/rants/gettingitright.htm) 4 May 2013 at the Wayback Machine by Jack Ganssle
121. Treglia, J., & Delia, M. (2017). Cyber Security Inoculation. Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY, 3–4 June.
122. Villasenor, John (2010). "The Hacker in Your Hardware: The Next Security Threat". *Scientific American*. **303** (2): 82–88. Bibcode:2010SciAm.303b..82V (https://ui.adsabs.harvard.edu/abs/2010SciAm.303b..82V). doi:10.1038/scientificamerican0810-82 (https://doi.org/10.1038%2Fscientificamerican0810-82). PMID 20684377 (https://pubmed.ncbi.nlm.nih.gov/20684377).
123. Waksman, Adam; Sethumadhavan, Simha (2010), "Tamper Evident Microprocessors" (https://web.archive.org/web/20130921055451/https://www.cs.columbia.edu/~waksman/PDFs/Oakland_2010.pdf) (PDF), *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, archived from the original (https://www.cs.columbia.edu/~waksman/PDFs/Oakland_2010.pdf) (PDF) on 21 September 2013, retrieved 27 August 2019
124. "Token-based authentication" (http://www.safenet-inc.com/multi-factor-authentication/authenticators/pki-usb-authentication/etoken-5200-token-based-authentication/). SafeNet.com. Archived (https://web.archive.org/web/20140320234026/http://www.safenet-inc.com/multi-factor-authentication/authenticators/pki-usb-authentication/etoken-5200-token-based-authentication/) from the original on 20 March 2014. Retrieved 20 March 2014.
125. "Lock and protect your Windows PC" (https://www.thewindowsclub.com/lock-protect-your-windows-pc-using-a-usb-drive-with-predator). TheWindowsClub.com. 10 February 2010. Archived (https://web.archive.org/web/20140320220321/http://www.thewindowsclub.com/lock-protect-your-windows-pc-using-a-usb-drive-with-predator) from the original on 20 March 2014. Retrieved 20 March 2014.
126. James Greene (2012). "Intel Trusted Execution Technology: White Paper" (http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf) (PDF). Intel Corporation. Archived (https://web.archive.org/web/20140611161421/http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf) (PDF) from the original on 11 June 2014. Retrieved 18 December 2013.
127. "SafeNet ProtectDrive 8.4" (http://www.scmagazine.com/safenet-protectdrive-84/review/2596/). SCMagazine.com. 4 October 2008. Archived (https://web.archive.org/web/20140320220133/http://www.scmagazine.com/safenet-protectdrive-84/review/2596/) from the original on 20 March 2014. Retrieved 20 March 2014.
128. "Secure Hard Drives: Lock Down Your Data" (https://www.pcmag.com/article2/0,2817,2342798,00.asp). PCMag.com. 11 May 2009. Archived (https://web.archive.org/web/20170621202140/http://www.pcmag.com/article2/0,2817,2342798,00.asp) from the original on 21 June 2017.
129. Souppaya, Murugiah P.; Scarfone, Karen (2013). "Guidelines for Managing the Security of Mobile Devices in the Enterprise" (https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise). *National Institute of Standards and Technology*. Special Publication (NIST SP). Gaithersburg, MD. doi:10.6028/NIST.SP.800-124r1 (https://doi.org/10.6028%2FNIST.SP.800-124r1).
130. "Forget IDs, use your phone as credentials" (http://video.foxbusiness.com/v/2804966490001/forget-ids-use-your-phone-as-credentials/?playlist_id=937116503001#sp=show-clips). Fox Business Network. 4 November 2013. Archived (https://web.archive.org/web/20140320215829/http://video.foxbusiness.com/v/2804966490001/forget-ids-use-your-phone-as-credentials/?playlist_id=937116503001#sp=show-clips) from the original on 20 March 2014. Retrieved 20 March 2014.

131. Lipner, Steve (2015). "The Birth and Death of the Orange Book". *IEEE Annals of the History of Computing*. **37** (2): 19–31. doi:10.1109/MAHC.2015.27 (https://doi.org/10.1109%2FMAHC.2015.27). S2CID 16625319 (https://api.semanticscholar.org/CorpusID:16625319).
132. Kelly Jackson Higgins (18 November 2008). "Secure OS Gets Highest NSA Rating, Goes Commercial" (http://www.darkreading.com/applications/secure-os-gets-highest-nsa-rating-goes-c/212100421). Dark Reading. Archived (https://web.archive.org/web/20131203031833/http://www.darkreading.com/applications/secure-os-gets-highest-nsa-rating-goes-c/212100421) from the original on 3 December 2013. Retrieved 1 December 2013.
133. "Board or bored? Lockheed Martin gets into the COTS hardware biz" (http://vita-technologies.com/articles/board-bored-lockheed-martin-co/). VITA Technologies Magazine. 10 December 2010. Archived (https://web.archive.org/web/20120502090205/http://vita-technologies.com/articles/board-bored-lockheed-martin-co/) from the original on 2 May 2012. Retrieved 9 March 2012.
134. Sanghavi, Alok (21 May 2010). "What is formal verification?". *EE Times_Asia*.
135. Ferraiolo, D.F. & Kuhn, D.R. (October 1992). "Role-Based Access Control" (http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf) (PDF). *15th National Computer Security Conference*: 554–563.
136. Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (August 1996). "Role-Based Access Control Models" (http://csrc.nist.gov/rbac/sandhu96.pdf) (PDF). *IEEE Computer*. **29** (2): 38–47. CiteSeerX 10.1.1.50.7649 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.50.7649). doi:10.1109/2.485845 (https://doi.org/10.1109%2F2.485845).
137. ABREU, VILMAR; Santin, Altair O.; VIEGAS, EDUARDO K.; STIHLER, MAICON (2017). *A multi-domain role activation model* (https://secplab.ppgia.pucpr.br/files/papers/2017-1.pdf) (PDF). *ICC 2017 2017 IEEE International Conference on Communications*. IEEE Press. pp. 1–6. doi:10.1109/ICC.2017.7997247 (https://doi.org/10.1109%2FICC.2017.7997247). ISBN 978-1-4673-8999-0. S2CID 6185138 (https://api.semanticscholar.org/CorpusID:6185138).
138. A.C. O'Connor & R.J. Loomis (March 2002). *Economic Analysis of Role-Based Access Control* (http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf) (PDF). Research Triangle Institute. p. 145.
139. "Studies prove once again that users are the weakest link in the security chain" (https://www.csoonline.com/article/2137210/security-awareness/studies-prove-once-again-that-users-are-the-weakest-link-in-the-security-chain.html). *CSO Online*. 22 January 2014. Retrieved 8 October 2018.
140. "The Role of Human Error in Successful Security Attacks" (https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/). *IBM Security Intelligence*. 2 September 2014. Retrieved 8 October 2018.
141. "90% of security incidents trace back to PEBKAC and ID10T errors" (https://www.computerworld.com/article/2910316/90-of-security-incidents-trace-back-to-pebkac-and-id10t-errors.html). *Computerworld*. 15 April 2015. Retrieved 8 October 2018.
142. "Protect your online banking with 2FA" (https://www.nzba.org.nz/2018/10/08/protect-your-online-banking-with-2fa/). *NZ Bankers Association*. 7 October 2018. Retrieved 7 September 2019.
143. "IBM Security Services 2014 Cyber Security Intelligence Index" (http://www.corporate-leaders.com/sitescene/custom/userfiles/file/White_Papers/Cyber_Security_Intelligence_Index.pdf) (PDF). 2014. Retrieved 9 October 2020.
144. Caldwell, Tracey (12 February 2013). "Risky business: why security awareness is crucial for employees" (https://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees). *The Guardian*. Retrieved 8 October 2018.

145. "Developing a Security Culture" (https://www.cpni.gov.uk/developing-security-culture). *CPNI - Centre for the Protection of National Infrastructure*.
146. "Cyber Hygiene – ENISA" (https://www.enisa.europa.eu/publications/cyber-hygiene). Retrieved 27 September 2018.
147. Kaljulaid, Kersti (16 October 2017). "President of the Republic at the Aftenposten's Technology Conference" (https://president.ee/en/official-duties/speeches/13671-president-of-the-republic-at-the-aftenpostens-technology-conference/index.html). Retrieved 27 September 2018.
148. Kuchler, Hannah (27 April 2015). "Security execs call on companies to improve 'cyber hygiene' " (https://www.ft.com/content/8468cfda-e9e3-11e4-a687-00144feab7de). *Financial Times*. Retrieved 27 September 2018.
149. "From AI to Russia, Here's How Estonia's President Is Planning for the Future" (https://www.wired.com/story/from-ai-to-russia-heres-how-estonias-president-is-planning-for-the-future/). *WIRED*. Retrieved 28 September 2018.
150. "Professor Len Adleman explains how he coined the term "computer virus" " (https://www.welivesecurity.com/2017/11/01/professor-len-adleman-explains-computer-virus-term/). *WeLiveSecurity*. 1 November 2017. Retrieved 28 September 2018.
151. "Statement of Dr. Vinton G. Cerf" (https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm). *www.jec.senate.gov*. Retrieved 28 September 2018.
152. Anna, Eshoo (22 May 2018). "H.R.3010 - 115th Congress (2017-2018): Promoting Good Cyber Hygiene Act of 2017" (https://www.congress.gov/bill/115th-congress/house-bill/3010). *www.congress.gov*. Retrieved 28 September 2018.
153. "Analysis | The Cybersecurity 202: Agencies struggling with basic cybersecurity despite Trump's pledge to prioritize it" (https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/07/26/the-cybersecurity-202-agencies-struggling-with-basic-cybersecurity-despite-trump-s-pledge-to-prioritize-it/5b58a84e1b326b1e64695548/). *The Washington Post*. Retrieved 28 September 2018.
154. "Protected Voices" (https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices). *Federal Bureau of Investigation*. Retrieved 28 September 2018.
155. "Incident Response Policy and Procedure | iCIMS" (https://www.icims.com/gc/incident-response-procedures/). *iCIMS | The Leading Cloud Recruiting Software*. Retrieved 13 March 2021.
156. Wilcox, S. and Brown, B. (2005) 'Responding to Security Incidents – Sooner or Later Your Systems Will Be Compromised', *Journal of Health Care Compliance*, 7(2), pp. 41–48.
157. Jonathan Zittrain, 'The Future of The Internet', Penguin Books, 2008
158. Information Security (https://fas.org/irp/gao/aim96084.htm) Archived (https://web.archive.org/web/20160306140354/http://fas.org/irp/gao/aim96084.htm) 6 March 2016 at the Wayback Machine. United States Department of Defense, 1986
159. "THE TJX COMPANIES, INC. VICTIMIZED BY COMPUTER SYSTEMS INTRUSION; PROVIDES INFORMATION TO HELP PROTECT CUSTOMERS" (http://www.businesswire.com/news/tjx/20070117005971/en) (Press release). The TJX Companies, Inc. 17 January 2007. Archived (https://web.archive.org/web/20120927014805/http://www.businesswire.com/news/tjx/20070117005971/en) from the original on 27 September 2012. Retrieved 12 December 2009.
160. Largest Customer Info Breach Grows (http://www.myfoxtwincities.com/myfox/pages/Home/Detail?contentId=2804836&version=3&locale=EN-US&layoutCode=TSTY&pageId=1.1.1) Archived (https://web.archive.org/web/20070928041047/http://www.myfoxtwincities.com/myfox/pages/Home/Detail?contentId=2804836&version=3&locale=EN-US&layoutCode=TSTY&pageId=1.1.1) 28 September 2007 at the Wayback Machine. MyFox Twin Cities, 29 March 2007.

161. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought" (http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11). *Business Insider*. 20 November 2013. Archived (https://web.archive.org/web/20140509020404/http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11) from the original on 9 May 2014.
162. Reals, Tucker (24 September 2010). "Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?" (http://www.cbsnews.com/8301-501465_162-20017507-501465.html). *CBS News*. Archived (https://web.archive.org/web/20131016133651/http://www.cbsnews.com/8301-501465_162-20017507-501465.html) from the original on 16 October 2013.
163. Kim Zetter (17 February 2011). "Cyberwar Issues Likely to Be Addressed Only After a Catastrophe" (https://www.wired.com/threatlevel/2011/02/cyberwar-issues-likely-to-be-addressed-only-after-a-catastrophe). *Wired*. Archived (https://web.archive.org/web/20110218154415/http://www.wired.com/threatlevel/2011/02/cyberwar-issues-likely-to-be-addressed-only-after-a-catastrophe/) from the original on 18 February 2011. Retrieved 18 February 2011.
164. Chris Carroll (18 October 2011). "Cone of silence surrounds U.S. cyberwarfare" (http://www.stripes.com/news/cone-of-silence-surrounds-u-s-cyberwarfare-1.158090). Stars and Stripes. Archived (https://web.archive.org/web/20120307021747/http://www.stripes.com/news/cone-of-silence-surrounds-u-s-cyberwarfare-1.158090) from the original on 7 March 2012. Retrieved 30 October 2011.
165. John Bumgarner (27 April 2010). "Computers as Weapons of War" (https://web.archive.org/web/20111219174833/http://www.crows.org/images/stories/pdf/IOI/IO%20Journal_Vol2Iss2_0210.pdf) (PDF). IO Journal. Archived from the original (http://www.crows.org/images/stories/pdf/IOI/IO%20Journal_Vol2Iss2_0210.pdf) (PDF) on 19 December 2011. Retrieved 30 October 2011.
166. Greenwald, Glenn (6 June 2013). "NSA collecting phone records of millions of Verizon customers daily" (https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order). *The Guardian*. Archived (https://web.archive.org/web/20130816045641/http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order) from the original on 16 August 2013. Retrieved 16 August 2013. "Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama"
167. Seipel, Hubert. "Transcript: ARD interview with Edward Snowden" (https://www.freesnowden.is/fr/2014/01/27/video-ard-interview-with-edward-snowden/). *La Foundation Courage*. Archived (https://web.archive.org/web/20140714174333/https://www.freesnowden.is/fr/2014/01/27/video-ard-interview-with-edward-snowden/) from the original on 14 July 2014. Retrieved 11 June 2014.
168. Newman, Lily Hay (9 October 2013). "Can You Trust NIST?" (https://spectrum.ieee.org/telecom/security/can-you-trust-nist). *IEEE Spectrum*. Archived (https://web.archive.org/web/20160201095426/https://spectrum.ieee.org/telecom/security/can-you-trust-nist) from the original on 1 February 2016.
169. "NIST Removes Cryptography Algorithm from Random Number Generator Recommendations" (https://www.nist.gov/itl/csd/sp800-90-042114.cfm). *National Institute of Standards and Technology*. 21 April 2014.
170. "New Snowden Leak: NSA Tapped Google, Yahoo Data Centers" (http://mashable.com/2013/10/30/nsa-google-yahoo-data-centers/) Archived (https://web.archive.org/web/20140709131535/http://mashable.com/2013/10/30/nsa-google-yahoo-data-centers/) 9 July 2014 at the Wayback Machine, 31 October 2013, Lorenzo Franceschi-Bicchierai, mashable.com

171. Michael Riley; Ben Elgin; Dune Lawrence; Carol Matlack (17 March 2014). "Target Missed Warnings in Epic Hack of Credit Card Data – Businessweek" (http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data). *Businessweek.com*. Archived (https://web.archive.org/web/20150127015928/http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data) from the original on 27 January 2015.
172. "Home Depot says 53 million emails stolen" (https://www.cnet.com/news/53-million-emails-stolen-in-home-depot-breach/). *CNET*. CBS Interactive. 6 November 2014. Archived (https://web.archive.org/web/20141209035159/http://www.cnet.com/news/53-million-emails-stolen-in-home-depot-breach/) from the original on 9 December 2014.
173. "Millions more Americans hit by government personnel data hack" (https://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709). *Reuters*. 9 July 2017. Archived (https://web.archive.org/web/20170228005352/http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709) from the original on 28 February 2017. Retrieved 25 February 2017.
174. Barrett, Devlin (4 June 2015). "U.S. Suspects Hackers in China Breached About four (4) Million People's Records, Officials Say" (https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888). *The Wall Street Journal*. Archived (https://web.archive.org/web/20150604215718/http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888) from the original on 4 June 2015.
175. Risen, Tom (5 June 2015). "China Suspected in Theft of Federal Employee Records" (https://web.archive.org/web/20150606064331/http://www.usnews.com/news/articles/2015/06/05/china-suspected-in-theft-of-federal-employee-records). *U.S. News & World Report*. Archived from the original (https://www.usnews.com/news/articles/2015/06/05/china-suspected-in-theft-of-federal-employee-records) on 6 June 2015.
176. Zengerle, Patricia (19 July 2015). "Estimate of Americans hit by government personnel data hack skyrockets" (https://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709). *Reuters*. Archived (https://web.archive.org/web/20150710075449/http://www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709) from the original on 10 July 2015.
177. Sanger, David (5 June 2015). "Hacking Linked to China Exposes Millions of U.S. Workers" (https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html). *The New York Times*. Archived (https://web.archive.org/web/20150605135158/http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html) from the original on 5 June 2015.
178. Mansfield-Devine, Steve (1 September 2015). "The Ashley Madison affair". *Network Security*. **2015** (9): 8–16. doi:10.1016/S1353-4858(15)30080-5 (https://doi.org/10.1016%2FS1353-4858%2815%2930080-5).
179. "Hackers Breached Colonial Pipeline Using Compromised Password" (https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password).
180. "Mikko Hypponen: Fighting viruses, defending the net" (http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html). TED. Archived (https://web.archive.org/web/20130116010603/http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html) from the original on 16 January 2013.
181. "Mikko Hypponen – Behind Enemy Lines" (https://www.youtube.com/watch?v=0TMFRO66Wv4). Hack in the Box Security Conference. Archived (https://web.archive.org/web/20161125075257/https://www.youtube.com/watch?v=0TMFRO66Wv4) from the original on 25 November 2016.

182. "Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information" (http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study). Government Accountability Office. Archived (https://web.archive.org/web/20151119221200/http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study) from the original on 19 November 2015. Retrieved 3 November 2015.
183. King, Georgia (23 May 2018). "The Venn diagram between libertarians and crypto bros is so close it's basically a circle" (https://qz.com/1284178/almost-half-of-cryptocurrency-and-bitcoin-bros-identify-as-libertarian/). *Quartz*.
184. Kirby, Carrie (24 June 2011). "Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cyber security" (http://articles.sfgate.com/2005-02-17/business/17361991_1_rsa-security-conference-cybersecurity-counterpane-internet-security). *The San Francisco Chronicle*.
185. McCarthy, Daniel (11 June 2018). "Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order" (https://doi.org/10.17645%2Fpag.v6i2.1335). *Politics and Governance*. **6** (2): 5–12. doi:10.17645/pag.v6i2.1335 (https://doi.org/10.17645%2Fpag.v6i2.1335).
186. "It's Time to Treat Cybersecurity as a Human Rights Issue" (https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue). *Human Rights Watch*. 26 May 2020. Retrieved 26 May 2020.
187. "FIRST Mission" (https://www.first.org/about/mission/). FIRST. Retrieved 6 July 2018.
188. "FIRST Members" (https://www.first.org/members/). FIRST. Retrieved 6 July 2018.
189. "European council" (http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp). Archived (https://web.archive.org/web/20141203223358/http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp) from the original on 3 December 2014.
190. "MAAWG" (http://www.maawg.org/about_maawg). Archived (https://web.archive.org/web/20140923153548/http://www.maawg.org/about_maawg) from the original on 23 September 2014.
191. "MAAWG" (http://www.maawg.org/about/roster). Archived (https://web.archive.org/web/20141017165203/http://www.maawg.org/about/roster) from the original on 17 October 2014.
192. "Government of Canada Launches Canada's Cyber Security Strategy" (http://www.marketwired.com/press-release/government-of-canada-launches-canadas-cyber-security-strategy-1328661.htm). *Market Wired*. 3 October 2010. Archived (https://web.archive.org/web/20141102175904/http://www.marketwired.com/press-release/government-of-canada-launches-canadas-cyber-security-strategy-1328661.htm) from the original on 2 November 2014. Retrieved 1 November 2014.
193. "Canada's Cyber Security Strategy" (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx). *Public Safety Canada*. Government of Canada. Archived (https://web.archive.org/web/20141102175701/http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx) from the original on 2 November 2014. Retrieved 1 November 2014.
194. "Action Plan 2010–2015 for Canada's Cyber Security Strategy" (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx). *Public Safety Canada*. Government of Canada. Archived (https://web.archive.org/web/20141102173436/http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx) from the original on 2 November 2014. Retrieved 3 November 2014.

195. "Cyber Incident Management Framework For Canada" (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-eng.aspx#_Toc360619104). *Public Safety Canada*. Government of Canada. Archived (https://web.archive.org/web/20141102213822/http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-eng.aspx#_Toc360619104) from the original on 2 November 2014. Retrieved 3 November 2014.
196. "Action Plan 2010–2015 for Canada's Cyber Security Strategy" (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx). *Public Safety Canada*. Government of Canada. Archived (https://web.archive.org/web/20141102173436/http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx) from the original on 2 November 2014. Retrieved 1 November 2014.
197. "Canadian Cyber Incident Response Centre" (http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx). *Public Safety Canada*. Archived (https://web.archive.org/web/20141008035436/http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx) from the original on 8 October 2014. Retrieved 1 November 2014.
198. "Cyber Security Bulletins" (http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/index-eng.aspx). *Public Safety Canada*. Archived (https://web.archive.org/web/20141008194739/http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/index-eng.aspx) from the original on 8 October 2014. Retrieved 1 November 2014.
199. "Report a Cyber Security Incident" (http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/rprt-eng.aspx). *Public Safety Canada*. Government of Canada. Archived (https://web.archive.org/web/20141111212708/http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/rprt-eng.aspx) from the original on 11 November 2014. Retrieved 3 November 2014.
200. "Government of Canada Launches Cyber Security Awareness Month With New Public Awareness Partnership" (http://www.marketwired.com/press-release/government-canada-launches-cyber-security-awareness-month-with-new-public-awareness-1706660.htm). *Market Wired*. Government of Canada. 27 September 2012. Archived (https://web.archive.org/web/20141103225408/http://www.marketwired.com/press-release/government-canada-launches-cyber-security-awareness-month-with-new-public-awareness-1706660.htm) from the original on 3 November 2014. Retrieved 3 November 2014.
201. "Cyber Security Cooperation Program" (http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-eng.aspx). *Public Safety Canada*. Archived (https://web.archive.org/web/20141102184754/http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-eng.aspx) from the original on 2 November 2014. Retrieved 1 November 2014.
202. "Cyber Security Cooperation Program" (http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-eng.aspx). *Public Safety Canada*. 16 December 2015. Archived (https://web.archive.org/web/20141102184754/http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-eng.aspx) from the original on 2 November 2014.
203. "GetCyberSafe" (http://www.getcybersafe.gc.ca/index-eng.aspx). *Get Cyber Safe*. Government of Canada. Archived (https://web.archive.org/web/20141111210737/http://www.getcybersafe.gc.ca/index-eng.aspx) from the original on 11 November 2014. Retrieved 3 November 2014.
204. "6.16 Internet security: National IT independence and China's cyber policy," in: Sebastian Heilmann, editor, ["China's Political System - Publications - About us - Mercator Institute for China Studies" (https://web.archive.org/web/20170323234015/https://www.merics.org/en/about-us/merics-analysis/chinas-political-system/). Archived from the original (https://www.merics.org/en/about-us/merics-analysis/chinas-political-system/) on 23 March 2017. Retrieved 11 May 2017. China*'s Political System*], Lanham, Boulder, New York, London: Rowman & Littlefield Publishers (2017) ISBN 978-1442277342

205. "Need for proper structure of PPPs to address specific cyberspace risks" (http://www.orfonline.org/cyfy-event/need-for-proper-structure-of-ppps-to-address-specific-cyberspace-risks/). Archived (https://web.archive.org/web/20171113165123/http://www.orfonline.org/cyfy-event/need-for-proper-structure-of-ppps-to-address-specific-cyberspace-risks/) from the original on 13 November 2017.
206. "National Cyber Safety and Security Standards(NCSSS)-Home" (https://www.ncdrc.res.in/). *www.ncdrc.res.in*.
207. "South Korea seeks global support in cyber attack probe". *BBC Monitoring Asia Pacific*. 7 March 2011.
208. Kwanwoo Jun (23 September 2013). "Seoul Puts a Price on Cyberdefense" (https://blogs.wsj.com/korearealtime/2013/09/23/seoul-puts-a-price-on-cyberdefense/). *The Wall Street Journal*. Dow Jones & Company, Inc. Archived (https://web.archive.org/web/20130925102342/http://blogs.wsj.com/korearealtime/2013/09/23/seoul-puts-a-price-on-cyberdefense/) from the original on 25 September 2013. Retrieved 24 September 2013.
209. "Text of H.R.4962 as Introduced in House: International Cybercrime Reporting and Cooperation Act – U.S. Congress" (https://web.archive.org/web/20101228170910/http://www.opencongress.org/bill/111-h4962/text). OpenCongress. Archived from the original (http://www.opencongress.org/bill/111-h4962/text) on 28 December 2010. Retrieved 25 September 2013.
210. [1] (http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123) Archived (https://web.archive.org/web/20120120040012/http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123) 20 January 2012 at the Wayback Machine
211. "Biden Adviser On Cyber Threats And The New Executive Order To Combat Them" (https://www.npr.org/2021/05/13/996617560/biden-advisor-on-cyber-threats-and-the-new-executive-order-to-combat-them). *NPR*.
212. Executive Order on Improving the Nation's Cybersecurity (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) (full text)
213. "National Cyber Security Division" (https://web.archive.org/web/20080611210347/https://www.dhs.gov/xabout/structure/editorial_0839.shtm). U.S. Department of Homeland Security. Archived from the original (https://www.dhs.gov/xabout/structure/editorial_0839.shtm) on 11 June 2008. Retrieved 14 June 2008.
214. "FAQ: Cyber Security R&D Center" (http://www.cyber.st.dhs.gov/faq.html). U.S. Department of Homeland Security S&T Directorate. Archived (https://web.archive.org/web/20081006042850/http://www.cyber.st.dhs.gov/faq.html) from the original on 6 October 2008. Retrieved 14 June 2008.
215. AFP-JiJi, "U.S. boots up cybersecurity center", 31 October 2009.
216. "Federal Bureau of Investigation – Priorities" (https://www.fbi.gov/about-us/quick-facts). Federal Bureau of Investigation. Archived (https://web.archive.org/web/20160711053557/https://www.fbi.gov/about-us/quick-facts) from the original on 11 July 2016.
217. "Internet Crime Complaint Center (IC3) – Home" (https://www.ic3.gov/default.aspx). Archived (https://web.archive.org/web/20111120021742/http://www.ic3.gov/default.aspx) from the original on 20 November 2011.
218. "Infragard, Official Site" (http://www.infragard.net/). *Infragard*. Archived (https://web.archive.org/web/20100909051004/http://www.infragard.net/) from the original on 9 September 2010. Retrieved 10 September 2010.

219. "Robert S. Mueller, III – InfraGard Interview at the 2005 InfraGard Conference" (https://web.archive.org/web/20110617004540/http://www.infragard.net/media/files/dir_med.mov). *Infragard (Official Site) – "Media Room"*. Archived from the original (http://www.infragard.net/media/files/dir_med.mov) on 17 June 2011. Retrieved 9 December 2009.
220. "CCIPS" (https://www.cybercrime.gov/). 25 March 2015. Archived (https://web.archive.org/web/20060823173821/http://www.cybercrime.gov/) from the original on 23 August 2006.
221. "A Framework for a Vulnerability Disclosure Program for Online Systems" (https://www.justice.gov/criminal-ccips/page/file/983996/download). Cybersecurity Unit, Computer Crime & Intellectual Property Section Criminal Division U.S. Department of Justice. July 2017. Retrieved 9 July 2018.
222. "Mission and Vision" (https://www.cybercom.mil/About/Mission-and-Vision/). *www.cybercom.mil*. Retrieved 20 June 2020.
223. "Speech" (http://www.defense.gov/speeches/speech.aspx?speechid=1399). Defense.gov. Archived (https://web.archive.org/web/20100415113237/http://www.defense.gov/speeches/speech.aspx?speechid=1399) from the original on 15 April 2010. Retrieved 10 July 2010.
224. Shachtman, Noah. "Military's Cyber Commander Swears: "No Role" in Civilian Networks" (http://www.brookings.edu/opinions/2010/0923_military_internet_shachtman.aspx) Archived (https://web.archive.org/web/20101106032102/http://www.brookings.edu/opinions/2010/0923_military_internet_shachtman.aspx) 6 November 2010 at the Wayback Machine, The Brookings Institution (http://www.brookings.edu/) Archived (https://web.archive.org/web/20060210001401/https://www.brookings.edu/) 10 February 2006 at the Wayback Machine, 23 September 2010.
225. "FCC Cybersecurity" (https://web.archive.org/web/20100527095750/http://www.fcc.gov/pshs/emergency-information/cybersecurity.html). FCC. Archived from the original (http://www.fcc.gov/pshs/emergency-information/cybersecurity.html) on 27 May 2010. Retrieved 3 December 2014.
226. "Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication" (https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm). *Food and Drug Administration*. Archived (https://web.archive.org/web/20160528153847/https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm) from the original on 28 May 2016. Retrieved 23 May 2016.
227. "Automotive Cybersecurity – National Highway Traffic Safety Administration (NHTSA)" (https://web.archive.org/web/20160525195552/http://www.nhtsa.gov/Research/Crash+Avoidance/Automotive+Cybersecurity). Archived from the original (https://www.nhtsa.gov/Research/Crash+Avoidance/Automotive+Cybersecurity) on 25 May 2016. Retrieved 23 May 2016.
228. Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen (http://www.gao.gov/products/GAO-15-370) (Report). U. S. Government Accountability Office. 14 April 2015. Archived (https://web.archive.org/web/20160613150636/http://www.gao.gov/products/GAO-15-370) from the original on 13 June 2016. Retrieved 23 May 2016.
229. Aliya Sternstein (4 March 2016). "FAA Working on New Guidelines for Hack-Proof Planes" (http://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/). *Nextgov*. Archived (https://web.archive.org/web/20160519181332/http://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/) from the original on 19 May 2016. Retrieved 23 May 2016.
230. Bart Elias (18 June 2015). "Protecting Civil Aviation from Cyberattacks" (https://www.fas.org/sgp/crs/homesec/IN10296.pdf) (PDF). Archived (https://web.archive.org/web/20161017100306/https://www.fas.org/sgp/crs/homesec/IN10296.pdf) (PDF) from the original on 17 October 2016. Retrieved 4 November 2016.

231. Verton, Dan (28 January 2004). "DHS launches national cyber alert system" (http://www.computerworld.com/securitytopics/security/story/0,10801,89488,00.html). *Computerworld*. IDG. Archived (https://web.archive.org/web/20050831162039/http://www.computerworld.com/securitytopics/security/story/0,10801,89488,00.html) from the original on 31 August 2005. Retrieved 15 June 2008.
232. Clayton, Mark (7 March 2011). "The new cyber arms race" (http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race). *The Christian Science Monitor*. Archived (https://web.archive.org/web/20150416090310/http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race) from the original on 16 April 2015. Retrieved 16 April 2015.
233. Nakashima, Ellen (13 September 2016). "Obama to be urged to split cyberwar command from NSA" (https://archive.today/20161012083815/https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html). *The Washington Post*. Archived from the original (https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html) on 12 October 2016. Retrieved 15 June 2017.
234. Overland, Indra (1 March 2019). "The geopolitics of renewable energy: Debunking four emerging myths" (https://doi.org/10.1016%2Fj.erss.2018.10.018). *Energy Research & Social Science*. **49**: 36–40. doi:10.1016/j.erss.2018.10.018 (https://doi.org/10.1016%2Fj.erss.2018.10.018). ISSN 2214-6296 (https://www.worldcat.org/issn/2214-6296).
235. Maness, Ryan C.; Valeriano, Brandon (11 June 2018). "How We Stopped Worrying about Cyber Doom and Started Collecting Data" (https://doi.org/10.17645%2Fpag.v6i2.1368). *Politics and Governance*. **6** (2): 49–60. doi:10.17645/pag.v6i2.1368 (https://doi.org/10.17645%2Fpag.v6i2.1368). ISSN 2183-2463 (https://www.worldcat.org/issn/2183-2463).
236. Maness, Ryan C.; Valeriano, Brandon (25 March 2015). "The Impact of Cyber Conflict on International Interactions". *Armed Forces & Society*. **42** (2): 301–323. doi:10.1177/0095327x15572997 (https://doi.org/10.1177%2F0095327x15572997). ISSN 0095-327X (https://www.worldcat.org/issn/0095-327X). S2CID 146145942 (https://api.semanticscholar.org/CorpusID:146145942).
237. Bullard, Brittany (16 November 2016). *Style and Statistics: The Art of Retail Analytics* (https://onlinelibrary.wiley.com/doi/book/10.1002/9781119271260) (1 ed.). Wiley. doi:10.1002/9781119271260.ch8 (https://doi.org/10.1002%2F9781119271260.ch8). ISBN 978-1-119-27031-7.
238. Oltsik, Jon (18 March 2016). "Cybersecurity Skills Shortage Impact on Cloud Computing" (http://www.networkworld.com/article/3045801/security/cybersecurity-skills-shortage-impact-on-cloud-computing.html). *Network World*. Archived (https://web.archive.org/web/20160323042705/http://www.networkworld.com/article/3045801/security/cybersecurity-skills-shortage-impact-on-cloud-computing.html) from the original on 23 March 2016. Retrieved 23 March 2016.
239. Robinson, Terry (30 May 2018). "Why is a Degree in Cyber Security one of the Best?" (https://www.degreequery.com/why-is-a-degree-in-cyber-security-one-of-the-best/). *DegreeQuery.com*. Retrieved 10 October 2021.
240. de Silva, Richard (11 October 2011). "Government vs. Commerce: The Cyber Security Industry and You (Part One)" (http://www.defenceiq.com/defence-technology/articles/the-cyber-security-industry-and-you/). Defence IQ. Archived (https://web.archive.org/web/20140424200253/http://www.defenceiq.com/defence-technology/articles/the-cyber-security-industry-and-you/) from the original on 24 April 2014. Retrieved 24 April 2014.
241. "Department of Computer Science" (https://web.archive.org/web/20130603085633/http://www.cs.gwu.edu/academics/graduate_programs/master/cybersecurity/cybersecurity-jobs). Archived from the original (http://www.cs.gwu.edu/academics/graduate_programs/master/cybersecurity/cybersecurity-jobs) on 3 June 2013. Retrieved 30 April 2013.

242. "About Cyber Security architect" (https://www.cisa.gov/security-architect). *cisa.gov*. 1 August 2021. Retrieved 1 January 2022.
243. Thomas, Jennifer (2 June 2021). "About Cyber Security Administrator (DPO)" (https://cybersguards.com/how-to-become-a-security-administrator/). *cybersguards.com*. Retrieved 4 January 2022.
244. "About Chief Information Security Officer (CISO) Carrer" (https://cybersecuritycareer.org/chief-information-security-officer-ciso/). *cybersecuritycareer.org*. 1 August 2021. Retrieved 4 January 2022.
245. "Data Protection Officers" (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/). *ico.org.uk*. January 2021.
246. KAGAN, JULIA (8 March 2021). "About Data Protection Officer (DPO)" (https://www.investopedia.com/terms/d/data-protection-officer-dpo.asp). *investopedia.com*. Retrieved 4 January 2022.
247. "Student Cybersecurity Resources" (https://niccs.cisa.gov/formal-education/students-launch-your-cyber-career). NICCS (US National Initiative for Cybercareers and Studies). Archived (https://web.archive.org/web/20201105234726/https://niccs.cisa.gov/formal-education/students-launch-your-cyber-career) from the original on 5 November 2020.
248. "Current Job Opportunities at DHS" (https://www.dhs.gov/join-dhs-cybersecurity). U.S. Department of Homeland Security. Archived (https://web.archive.org/web/20130502135412/http://www.dhs.gov/join-dhs-cybersecurity) from the original on 2 May 2013. Retrieved 5 May 2013.
249. "Cybersecurity Training & Exercises" (https://www.dhs.gov/cybersecurity-training-exercises). U.S. Department of Homeland Security. 12 May 2010. Archived (https://web.archive.org/web/20150107111146/http://www.dhs.gov/cybersecurity-training-exercises) from the original on 7 January 2015. Retrieved 9 January 2015.
250. "Cyber Security Awareness Free Training and Webcasts" (https://msisac.cisecurity.org/resources/videos/free-training.cfm). MS-ISAC (Multi-State Information Sharing & Analysis Center). Archived (https://web.archive.org/web/20150106064140/http://msisac.cisecurity.org/resources/videos/free-training.cfm) from the original on 6 January 2015. Retrieved 9 January 2015.
251. "DoD Approved 8570 Baseline Certifications" (https://web.archive.org/web/20161021073353/http://iase.disa.mil/iawip/Pages/iabaseline.aspx). *iase.disa.mil*. Archived from the original (http://iase.disa.mil/iawip/Pages/iabaseline.aspx) on 21 October 2016. Retrieved 19 June 2017.
252. "The UK Cyber Security Strategy: Report on Progress and Forward Plans December 2014" (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf) (PDF). United Kingdom Cabinet Office. Archived (https://web.archive.org/web/20180418230804/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf) (PDF) from the original on 18 April 2018. Retrieved 20 August 2021.
253. "Cyber skills for a vibrant and secure UK" (https://www.gov.uk/government/news/cyber-skills-for-a-vibrant-and-secure-uk).
254. "Singapore Operational Technology (OT) Cybersecurity Competency Framework" (https://www.csa.gov.sg/News/Press-Releases/singapore-operational-technology-cybersecurity-competency-framework).
255. "Confidentiality" (http://medical-dictionary.thefreedictionary.com/confidentiality). Retrieved 31 October 2011.

256. "Data Integrity" (http://www.businessdictionary.com/definition/data-integrity.html). Archived (https://web.archive.org/web/20111106055944/http://www.businessdictionary.com/definition/data-integrity.html) from the original on 6 November 2011. Retrieved 31 October 2011.
257. "Endpoint Security" (http://www.webopedia.com/TERM/E/endpoint_security.html). 10 November 2010. Archived (https://web.archive.org/web/20140316021605/http://www.webopedia.com/TERM/E/endpoint_security.html) from the original on 16 March 2014. Retrieved 15 March 2014.

Further reading

- Jeremy Bob, Yonah (2021) "Ex-IDF cyber intel. official reveals secrets behind cyber offense (https://www.jpost.com/israel-news/ex-idf-cyber-intel-official-how-to-carry-out-a-cyber-offense-attack-677173)". The Jerusalem Post (https://www.jpost.com/)
- Branch, J. (2020). "What's in a Name? Metaphors and Cybersecurity. (https://www.cambridge.org/core/journals/international-organization/article/whats-in-a-name-metaphors-and-cybersecurity/563998100A2FAF1E5DFDB5C52EC68569)" *International Organization.*
- Costigan, Sean; Hennessy, Michael (2016). *Cybersecurity: A Generic Reference Curriculum* (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf) (PDF). NATO. ISBN 978-9284501960.
- Fuller, Christopher J. "The Roots of the United States' Cyber (In)Security," *Diplomatic History* 43:1 (2019): 157–185. online (https://eprints.soton.ac.uk/407741/3/Fuller_Roots_of_Cyber_Insecurity_clean_images.doc)
- Kim, Peter (2014). *The Hacker Playbook: Practical Guide To Penetration Testing*. Seattle: CreateSpace Independent Publishing Platform. ISBN 978-1494932633.
- Lee, Newton (2015). *Counterterrorism and Cybersecurity: Total Information Awareness* (2nd ed.). Springer. ISBN 978-3319172439.
- Montagnani, Maria Lillà and Cavallo, Mirta Antonella (26 July 2018). "Cybersecurity and Liability in a Big Data World (https://ssrn.com/abstract=3220475)". SSRN.
- Singer, P. W.; Friedman, Allan (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. ISBN 978-0199918119.
- Wu, Chwan-Hwa (John); Irwin, J. David (2013). *Introduction to Computer Networks and Cybersecurity*. Boca Raton: CRC Press. ISBN 978-1466572133.
- M. Shariati et al. / Procedia Computer Science 3 (2011) 537–543. Enterprise information security, a review of architectures and frameworks from interoperability perspective (https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050911X00029/1-s2.0-S1877050910004643/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEIj%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIQD4z1%2FUFlsy48bnmhCRAIejgyz1XGFVk2KasfEIfqGFoAIgaSQeYUBiUfA9CAtz9wFRcNq138Koa5ar8AVdEyxgfTAqtAMIlRACGgwwNTkwMDM1NDY4NjUiDAPP%2FPtzMzddVxNW4CqRAxoaT4FbZhW6JGW31Sm757WEv5wraQtcE4hcB1BU44CdVV4MuCoiNmuORpy9MDgvg2JU%2BHf6qpDJSWsUZdCoehp%2FMUvGJsR42VlliPnndECLtZONMiq5Ie%2BhjlZU3i8nd8shf2gaSHeQW0bWt1a%2FdLxcFv4ynkTTrMGGLCBJPJMG0k1oab97mliUqW86wlUS7Vr4aw7yCAHvkXjMIXnUvAJYGsAZljDnvKmSc7cy4XY5OvraUALCHZg38hvvcbM4AySzr8QYu6kPxPVMFhgC8ucTrDFHSRKYU1JiiaS32vF2QMFH0gqYtXTqbMetaNAei0yvxYNPY%2BCpOnwLkEXvPX0mJmHbf9aqx1TeLPbCj%2Bk8fPcVi0bzbnuJ3Yr6T2Kb0%2F5oc1tOUemsQEuZKTujmcKuUkbPpgOA2J8EEXkU2bzHFy5Fhv105P2N6YHG9%2BFcN2RAkfr9mRIlo0w4OauDmxG5BxJYKQT80FtDSLBDXMmUijDOR3EKfFmzXci9dq9JhkQ0bawLiGVGf2jS3dhfBNs5MPOenvEFOusBI0qKDfyJmskyM%2FReHn%2BcE3eNaSukcQrKYbXlncPZJB8%2BzCkGSjSy8T7NHJ839ZTa9iEvV%2BEz3ExRY0KyNL%2FLhxkX6tCzz5BqV1aTnavq1GfvjClfGrhTVFUovlTQ78vyBbP6n56R2ARW99MVMlzX43KswXkk969lJUR9qunXJfehOfzOeaXc1Y5hMotfm4mlljsGdqB5JJR%2F0rJoI1gbr4axVp5Z43wDzEmGm3QhK7PWP4Nc93O04C5dJ9uiBDd%2FXplsoE8KFuJ7cFQh3pOMFhhWWnzj3wofZnNhT6Yl9OjDda6lhQ6Yq0bP%2Bw%3D%3D&X-Amz-

Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20200122T002111Z&X-Amz-SignedHeaders=host&X-Amz-Expires=300&X-Amz-Credential=ASIAQ3PHCVTYXFDHEAEB%2F20200122%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=ee4f4894260b36442dce7dd30417a57f87f6101f364bc7211871146034695688&hash=e90a3374f116a057e0417cb153f7e1984a4115e1eb04e1394465765a9bf7fc26&host=68042c943591013ac2b2430a89b270f6af2c76d8dfd086a07176afe7c76c2c61&pii=S1877050910004643&tid=spdf-0ae4086a-ca27-45fb-bcb6-442da89c5115&sid=6cb434c84545c44875084095905ab341a297gxrqa&type=client)
