IMT 500
Jacob Kovacs
10/20/2016

Information security analysis

What is information security?

Information is an important organizational asset that requires protection. The technological specifics of information threats have changed over the years—from solo hacker-written viruses in the 1980s to cybercrime cartels in the 1990s, from government- or business-backed cyberattacks of the present to whatever comes next (Tanz, 2016)—but the scope of information security can be summarized quickly[1] as the 'CIA triad' of confidentiality, integrity, and availability. Each term means something specific. *Confidentiality* means data is private, accessible only to authorized users; *integrity* refers to data that is protected from unwanted modification or deletion; *availability* means keeping computing resources running despite power outages, hardware failure, system upgrades, software bugs, and wide variation in network traffic (Perrin, 2008).

Attacks against information systems are highly diverse and can be classified in many ways. In terms of intended impact, attacks may attempt to destroy or crash a system; to hold a system hostage; to sap or divert system resources, perhaps in the process of committing a further crime against another target; to steal information for misuses like blackmail, identify theft, and fraud; or to outright steal money. These impacts may be achieved through many different channels[2], with the list subject to endless innovation. Schiff (2015) summarizes some of the major vulnerabilities companies face, as well as some necessary defensive measures:

- *Disgruntled or careless employees* can steal information or endanger it through poor use of company devices (e.g., weak passwords, accidental malware installation, browsing bad sites). Companies can keep permissions current; log and monitor users; use an intrusion detection system (IDS); train employees; encrypt network traffic; use sophisticated authentication schemes (digital certificate, multifactor authentication, biometric authentication); and use a password management system.
- *Bring your own device (BYOD) computing*—where employees expect to use their personal devices on the company network, or to access company resources through their personal network—makes an information security professional's job much harder by introducing many more potential sites for vulnerabilities. This risk can be ameliorated with BYOD policies, containerization of devices, constant monitoring by an IDS, and use of cloud services as a buffer.
- *Weak links in the network* arise when devices can no longer be patched. Someone must monitor the support status of devices and be ready to outdated ones.

[1] The CIA triad is a simple starting point but it is not exhaustive. After extensive review of literature from the neighboring disciplines of computer security, information security, and information assurance, Cherdantseva and Hilton (2014) define information security in terms of "security goals" and "security mechanisms". The three elements of the CIA triad are considered security goals, and Cherdantseva and Hilton identify many others in their synthesis—namely *accountability, assurance, authentication, non-repudiation, authenticity, reliability, effectiveness, efficiency, compliance, utility, possession, control, authorisation, awareness, access, identification, accuracy, administration, classification, anonymity, audit,* and *safety.*

[2] Too many to define, but here's a list of them adapted from Raj (n.d.): *phishing; malware (ransomware, keylogging software); denial of service (DoS) through network bandwidth consumption; DoS through resource starvation (email bombs, ping flood attacks/smurfing, teardrop attacks, bogus return addresses); DoS by taking advantage of a software bug; DoS through routing/DNS attacks, which exploit poor router security (DDoS, eavesdropping, active attacks, spoofing, replay attacks, packet alteration); DoS through application-level attacks (viruses, cookie poisoning, hidden-field manipulation, parameter tampering, buffer overflow, cross-site scripting, backdoor and debug options that are left in software accidentally, forceful browsing, stealth commanding, third-party misconfiguration, and password cracking including screen saver passwords).*

- *Negligent or malicious contractors and third-party services* can undermine a system's security when backdoors are intentionally left in software; when remote vendor access channels are exploited; or when data stored on the client's behalf is not encrypted. Security professional Adam Roth (quoted in Schiff, 2015) notes that "data breach typically does not directly attack the most valuable server, but is more a game of [leapfrog], going from a low level computer that is less secure, then pivoting to other devices and gaining privileges". Companies can guard this risk vector by investigating vendor security practices, then monitoring their activity in readiness to cut them off.

Many of Schiff's identified vulnerabilities and countermeasures pertain to *confidentiality*, the protection of private data. *Integrity* is secured through system backup and version control, while *availability* is ensured through scheduled maintenance and cloud backup, among other strategies. Security solutions can also be classified by *layer* in what's called the 'defense in depth' approach or the 'onion model' (Steinklauber, 2015; Wikipedia, 2016):

- The *logical* or technical layer: protect networks with switches, firewalls, etc.; protect phone systems with encryption; protect operating system with anti-virus software; etc.
- The *physical* layer: areas, rooms, or machines can be physically locked or restricted.
- The *administrative* or procedural layer: policies, regulations, guidelines, and training can be applied to modify the behavior of human users.

Information security is important

Thinking of MSIM students, information security is relevant to all of us regardless of specialization. In future managerial and leadership roles, we will *all* want to keep products working properly, meet our legal obligations, retain proprietary information that confers a competitive advantage, etc., and all of these tasks depend on the security of underlying information and information technology. Specializations where information security is particularly complementary include information consulting (where it will be a common client request) as well as business intelligence and data science (which both require valid data as input in order to yield valid insights as output).

Information security trends

Security technologist Bruce Schneier makes the point that every advance in our technological capability comes with a security price tag (RSA Conference, 2016). With increased collection of consumer data for 'good' purposes comes higher risk of dangerous privacy violations, surveillance, and blackmail. With the massive 'availability' gains of the cloud comes greater risk of 'confidentiality' and 'integrity' violations. The addition of computing to everyday devices (IoT) inducts novel human activities to the realm of information security at the same time it facilitates and improves those activities.

Two expert reviews of the information security horizon (Gill, 2015; Olavsrud, 2015) agree on the growing salience of IoT- and BYOD-related vulnerabilities (device identities are easy to spoof, hard to authenticate); of government- or organization-sponsored cyberattacks; of Big Data breaches; and of increasingly sophisticated cybercrime that targets universal technologies and protocols (SSL, Bash) as well as specific companies in highly tailored fashion. In addition to these trends, I'll mention the competing economic and political pressures that companies will face in the information security arena. Governments have sought backdoors and surveillance privileges in new technology for years (RSA Conference, 2016), but a recent news item (Levin, 2016) illuminates the present scope of the issue: "Half of US adults"—over 117 million people—are recorded in police facial recognition databases". Consumers, meanwhile, will fight for data privacy so long as they *know about* threats. I expect to see many cycles of companies caving to government pressure, followed by consumer outrage and belated political activism to curtail the exposed practices.

References

Cherdantseva, Y. & Hilton, J. (2014). Information security and information assurance. In F. Almeida & I. Portela (eds.), *Organizational, legal, and technological dimensions of information system administration*. Hershey, PA: IGI Global Publishing. Retrieved from http://www.igiglobal.com/chapter/information-security-and-information-assurance/80717

Gill, T. (2015, December 8). 2016's top information security threats. *Continuity Central.* Retrieved from http://www.continuitycentral.com/index.php/news/technology/729-2016-s-top-information-security-threats

Levin, S. (2016, October 18). Half of US adults are recorded in police facial recognition databases, study says. *The Guardian.* Retrieved from https://www.theguardian.com/world/2016/oct/18/police-facial-recognition-database-surveillance-profiling

Olavsrud, T. (2015, December 21). 5 information security trends that will dominate 2016. *CIO*. Retrieved from http://www.cio.com/article/3016791/security/5-information-security-trends-that-will-dominate-2016.html

Perrin, C. (June 30, 2008). The CIA triad. TechRepublic. Retrieved from http://www.techrepublic.com/blog/it-security/the-cia-triad/

Raj, P. (n.d.). Information security: Challenges and solutions. Retrieved from http://www.peterindia.net/ITSecurityView.html

RSA Conference. (2016, March 1). 2016: 25 years of information security [Video file]. Retrieved from https://www.youtube.com/watch?v=oIbl1jVUkJs

Schiff, J. L. (2015, January 20). 6 biggest business security risks and how you can fight back. *CIO*. Retrieved from http://www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html

Steinklauber, K. (2015, January 15). Data security defense in depth: The onion approach to IT security. *SecurityIntelligence.* Retrieved from https://securityintelligence.com/data-security-defense-in-depth-the-onion-approach-to-it-security/

Tanz, J. (2016, October 18). Hey Silicon Valley: President Obama has a to-do list for you. *Wired.* Retrieved from https://www.wired.com/2016/10/obama-six-tech-challenges/

Wikipedia. (2016, October 10). Defense in depth (computing). Retrieved from https://en.wikipedia.org/w/index.php?title=Defense_in_depth_(computing)&oldid=743567628