International Journal of Applied Technology & Leadership
ISSN 2720-5215
Volume 1, Issue 1, January 2022
ijatl@org

Time Factors in Risk Management Decisions

Paul Cheney, Capitol Technology University

Ian R. McAndrew PhD, Capitol Technology University

Abstract
Coronavirus has been a driving force of cyber-attacks, by virtue of phishing attacks. The new work pattern of working from home and uncertainty has increased risks. However, like the effects of COVID-19, the risks and vulnerability created by the rapid shift of society to working from home out of necessity has created unparalleled risks. The rapid move to working from home does not have a commiserate level of protection on the home or the business side of the network. Research in cell phones, home electronics and vulnerabilities of all types of computers, have combined to create a perfect storm of long-term damage and access to corporate and home networks alike. This paper will demonstrate that additional factors should be taken into account at the core risk decision making process as well as how risk methodologies are used

Index Terms
Risk Management, Critical Infrastructure, Failure Modes, Effect Analysis, Detection, Monitoring

Introduction

Coronavirus has been a driving force of cyber attacks, and phishing attacks have been one of the main and easiest ways for cyber criminals. Indeed, this has not been the only way, just the simplest to maximize the success for those with nefarious aims. However, like the effects of COVID-19, the risks and vulnerability created by the rapid shift of society to working from home out of necessity has created unparalleled risks. These changes have highlighted views of our networks as fluid and more importantly the changing security assumptions. Virtual Private Networks (VPNs) changes have moved and layered perimeters. Security is implemented in numerous layers through a computer system and network. Using the Open Systems Interconnection (OSI) model can focus on different layers: one example would be having a network firewall and a client

firewall. If one were to fail, the other could potentially still block attacks. Security is the building up of these layers across every level of the system of systems.

This paper will demonstrate that additional factors should be taken into account at the core risk decision making research in cell phones, home electronics and vulnerabilities of all types of computers, have combined to create a perfect storm of long term damage and access to corporate and home networks alike. Furthermore, the research will include those associated risks and practices that may need to be included accordingly. This research is reporting initial findings for longer term study of research in the subject.

The advantage of time is for the Attackers, but enables Defense

The advantage of time is in the favor of attackers. Not only do attackers have unlimited time for attacks, but they are not bound by development time. Corporations with long development lead times are particularly susceptible to blackmail and loss of confidentiality attacks. For example, game developers may spend ten plus years building a game and if it is compromised in that time, they will lose all profits from the game, so they are particularly susceptible to blackmail or extortion. The Defender's inherent advantage is knowing the environment and the systems. However, the engineering and operation rigor required to fully take advantage of home field advantage is commonly not implemented due to network and human resource constraints. Additionally, upon detection of any abnormal behavior it will be hard to identify due to the common development methodologies: where development teams have reorganized or dispersed after a system is fielded. This problem is more apparent when third party contractors or external developers are used. Without detailed knowledge of the system and without a common known good baseline detection and identification of malware or malicious behavior will be extremely difficult.

Radical Sociological Changes drive technical Risks

Because of the global pandemic, radical changes have happened that impacts how work is done. These changes include emergency needs to increase VPN remote work capability and capacity. These changes in capacity have often broken or break architectural and engineering security assumptions. These assumptions form the basis for security of systems and yet business needs override and break these security models. For example, security tools might need to send a report to the management center, but because of the bandwidth of working remotely, these might take longer to come in. Additionally, users may not have the necessary bandwidth and may slow security response. Split Tunnel VPNs used to save server bandwidth is the equivalent to having an endpoint in the user’s home network, without additional mitigations.

Supply Chains are Inherited Risks but not Inherited Controls

Software and hardware supply chain attacks are on the rise with SolarWinds being the most blatant and critical Epoch event. The damage from these attacks, particularly due to the attacker access to Solar Winds and the nature of access that SolarWinds has, is incalculable. Additionally, the cost of not only the investigation but remediation could easily run hundreds of millions of dollars. At what point do you give up confidentiality of data in order to maintain integrity and availability? With the attacker's skill level, it is not out of the realm of possibility that they have deep level persistence across various compromised networks including Department of Homeland Security, Treasury, and Commerce. Additionally, the attackers' visibility into the cyber security firm FireEye almost certainly have given the attackers early warning to change command and control and related malware packages and other indicators of compromise. The cost incurred by this attack is intangible

Independent Identification of IOCs is possible but very hard

Identification of malicious activity using IOCs required prior identification of the IOCs. IOCs can readily be changed by the attacker and it is silly to believe that this methodology scales. The time frame of detection vs. the time frame for changing IOCs is asymmetrically in favor of the attacker. In order to defend attacks, negative set subtraction such that the behavior of a system minus the known good of the system equates to bad activity or not understood activity. The risk management framework does not clearly highlight this manner of detection that works across all systems processes verticals.

Integrity of Data

Damage to code, software and hardware can induce and drive further risks. Supply chain attacks, SolarWinds[11] and the attempted PHP Attack[12] show the value of targeting upstream providers. New research into Dependence Confusion attacks, shows that there is exponential value in exploitation. The higher up the dependency chain you attack, the more value is gained for the attackers. Instead of hacking one target and getting the value of that one hack, The hackers instead gain access to multiple targets. Additionally these attacks are harder to detect because operators trust the security of their vendors, and open source repositories. What is the damage if supply chain attacks are executed against crucial software that drives Critical Infrastructure? The damage of Stuxnet has highlighted the damage that alterations of software can cause [13]. The Saudi Aramco attacks purpose was to incur the maximum monetary damage possible. Imagine where the purpose is the loss of human life and chaos. Human lives may have already been lost due to the plague of ransomware[14]. If lives have not been loss due to ransomware, they have been lost

because of software glitches. Flight Software on the Boeing 747MAX and the Therac 25 are often quoted examples. What happens when death becomes the goal?

Protection vs Detection

Locard's exchange principle dictates that an attacker will leave something behind. Zero days guarantee that all attacks cannot be prevented. However network administrators are able to monitor the behavior of systems. In theory a system should always be able to be monitored for changes that are both indicative of an attack or another issue. There is a trade off to be made in attack prevention where money is spent: security comes from preventing common attacks they are bad enough to care about. The current risk measurement or calculation is Likelihood of Occurrence * Severity. However this formula does not take the difference into account between prevention and detection of whatever mitigations are emplaced to stop the attack.

The average time an attacker is in a network undetected is 56 days[8]. That means prevention of attacks is not working and probably has not been for many years leaving the problem of legacy concerns. It is untenable to believe that protection alone is enough as prevention has to be achieved, and many argue that protections must be built in and not added. Thus, it means that detection is required that is of the highest probability of success and reliability. In order to enable protection detection of threats, it requires that proper engineering and architecture be implemented. Since reengineering a network in place is often impractical, this highlights the importance of proper engineering practice the first time. However, since threats evolve, any network must be able to flex to future requirements of detection. Since the defenders have home field advantage, strong monitoring and process knowledge is required for secure monitoring and cyber threat detection.

Humans are ill suited for risk analysis of technology. Humans are good at facing the current circumstances; however, humans do not like to think that someone is out to get us, and the constant wear of threat tends to reduce the seriousness that people view possible attacks[4]. The Risk Management Framework (RMF) by the National Institute of Standards and Technology headquartered in Gaithersburg, MD. sets standards and definitions used by The United States Government. Additionally, reference “Categorizing Threat: Building and Using a Generic Threat Matrix” to highlight critical flaws that arise when strictly following the RMF from NIST.

Hackers are good at constant reevaluation. They limit the circumstances to where they are currently looking, so it’s much easier for an attacker to evolve their methodology, that is employed over and over across various targets than it is for a defender to re-architect the network and everything that relies on its function and security. Security at every layer in the Open Systems Interconnectability (OSI) stack must follow the rules of a reference monitor, must be always invoked and non-bypassable. Most networks are multiple levels whether designed that way or not. There are administrators and users. It is a fact that security of any computing system is enforced by reference monitor type access, common examples being Bell–LaPadula and Clark–Wilson models.

Ransomware and the information leakage attacks are new avenues that undercut the nature of security by giving attackers leverage over common business methods to manage publicity. For

Example knowing the business cases for security during a CISSP examination, these new attacks attack the business foundation which is the reason that ransomware attacks in particular are paying out at a much higher rate than previous attacks; it is an attack on the business and not on the information itself. Businesses have a vested interest in the public not knowing they have been hacked for legal and publicity reasons. Common business methods of preventing identification of compromise preclude that secrecy by demonstrating the breach OR directly prevent the business from operation.
Garmin is a huge company in the market of navigation equipment, but of particular concern is the navigation systems in personal aircraft, such as the G-1000 and G-3000 systems. Was the code of these devices stolen? Was the code signing certificates used to update these systems stolen? Do you trust Garmin systems any less because of the hack? Garmin reportedly paid a 10-million-dollar ransom. That means if these hackers reinvested that money, they could buy several new Zero-day vulnerabilities and create havoc across a much broader market. Payments to ransomware actors are usually in violation of US law[9], it is often recommended by insurance companies.

The Saudi Aramco attack with permanent damage to infrastructure has highlighted the cost. Hackers behind attacks that could cost human life have been sanctioned [10]. The Triton malware is the first SCADA malware that was designed to circumvent safety mechanisms and enable the direct taking of human life by the interruption of proper operation of the SCADA system.

YouTube and Raspberry Pi-s have lowered the bar for attackers to learn and conduct complex attacks previously exclusive to Governments and well-funded organizations. YouTube is not only used for information warfare, but significantly lowering the skill floor needed for attackers. Script kiddies are now empowered by the simplicity of new attacks as well as the ability to learn and execute new skills.

Google uses a ‘Zero-Trust’ network model. This model focuses on decentralized networks and ensuring good network separation as well as data over APIs. These APIs act as reference monitors and allow for strict logging and monitoring. The Zero-Trust model works very well for future proofing. This model allows for good security and strong flexibility. Any network operating under this model would be well suited to the type of fundamental shift, similar to the one caused by COVID-19 .$\text{Discipline} = \text{Security}, \text{Discipline} = \text{Assurance}.$
Some models of security cost more to implement than others. Zero-Trust security model is one of those models which costs more to implement, but has significant advantages over traditional “hard outside, soft inside models”.

Conclusion

As hard drives grow, the space we use also grows. This means more files, which potentially have flaws, backdoored programs which are only discovered years down the road. This means more software that has flaws installed and present on the machine. More time gives a greater likelihood of a supply chain compromise of the software compilation chain. More time means it is likely that any one password has been compromised.

In order to maintain the same level of security over time, more and more investment must be made into security.

$$\text{Risk} = \text{Likelihood x Severity}$$
$$\text{Likelihood} = \text{Vulns} * \text{Threats}$$

Looking at the above equations we can see that

$$\text{Risk} = \text{Vulns} * \text{Threats} * \text{Severity}.$$

The number of vulnerabilities increases over time, so risks increase over time by nature of running with a 'normal' IT system.

Threats increase over time, as skill levels required for more advanced techniques drop.

Supply chain attacks are growing. The software supply chain attack executed against SolarWinds enabled access to potentially tens of thousands of other networks. Imagine if ransomware or a wiper malware was deployed, large numbers of corporations across many sectors would be instantly crippled. The more sinister thing is the manner in which the attack was executed against the victims. Even if the victims tested and waited to deploy patches, it would have done no good. The malware waited almost 2 weeks to beacon out. Attack persistence mechanisms have altered as technology changes particularly with new subsystems such as UEFI. New persistence mechanisms using UEFI for deep level persistence have not only been discovered but code taking advantage is also publicly available. Due to the nature of these deep level persistence mechanisms, it can be impossible to detect, much less remediate, due to the design and implementation of these systems. A common example is detection of bad USB devices. Where you ask for a copy of the running firmware on the device and it returns a known good object while itself running malicious code. The only manner to detect such an attack would be deep level forensic analysis of either memory or hardware.

REFERENCES

[1] J. Dunagan, A. Zheng, and D. R. Simon, "Heat-ray: Combating Identity Snowball Attacks Using Machine Learning, Combinatorial Optimization and Attack Graphs," Jan. 2009 [Online]. Available: https://www.microsoft.com/en-us/research/publication/heat-ray-combating-identity-snowball-attacks-using-machine-learning-combinatorial-optimization-and-attack-graphs/. [Accessed: 29-Aug-2020]

[2] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15, 2002, pp. 49–63, doi: 10.1109/CSFW.2002.1021806.

[3] "28 health system cyberattacks, data breaches so far in 2020." https://www.beckershospitalreview.com/cybersecurity/28-health-system-cyberattacks-data-breaches-so-far-in-2020.html (accessed Aug. 29, 2020).

[4] N. Bodemer, A. Ruggeri, and M. Galesic, "When Dread Risks Are More Dreadful than Continuous Risks: Comparing Cumulative Population Losses over Time," PLoS ONE, vol. 8, no. 6, pp. 1–6, Jun. 2013, doi: 10.1371/journal.pone.0066544.

[5] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, NIST SP 800-53r4, Apr. 2013. doi: 10.6028/NIST.SP.800-53r4.
[6] L. Woodard, C. K. Veitch, S. R. Thomas, and D. P. Duggan, "Categorizing threat : building and using a generic threat matrix.," SAND2007-5791, 921121, Sep. 2007. doi: 10.2172/921121.
[7] John Lambert, "Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win." https://docs.microsoft.com/en-us/archive/blogs/johnla/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win (accessed Sep. 02, 2020).
[8] "[Report] M-Trends 2020," FireEye. content.fireeye.com (accessed Sep. 07, 2020).
[9] Krebs, "Ransomware Victims That Pay Up Could Incur Steep Fines from Uncle Sam," Brian Krebs, 01-Oct-2020. [Online]. Available: https://krebsonsecurity.com/2020/10/ransomware-victims-that-pay-up-could-incur-steep-fines-from-uncle-sam/. [Accessed: 26-Oct-2020].
[10] D. Goodin, "Hackers behind life-threatening attack on chemical maker are sanctioned," Ars Technica, 23-Oct-2020. [Online]. Available: https://arstechnica.com/information-technology/2020/10/us-sanctions-russian-hackers-who-hit-chemical-maker-with-dangerous-malware/. [Accessed: 26-Oct-2020].
[11] "SolarWinds Breach Used to Infiltrate Customer Networks (Solarigate)," SANS Internet Storm Center, Mar. 29, 2021. https://isc.sans.edu/forums/diary/26884 (accessed Mar. 29, 2021).
[12] D. Goodin, "Hackers backdoor PHP source code after breaching internal git server," Ars Technica, Mar. 29, 2021. https://arstechnica.com/gadgets/2021/03/hackers-backdoor-php-source-code-after-breaching-internal-git-server/ (accessed Mar. 31, 2021).
[13] "Stuxnet Worm Attack on Iranian Nuclear Facilities." http://large.stanford.edu/courses/2015/ph241/holloway1/ (accessed Mar. 31, 2021)
[14] "Ransomware did not kill a German hospital patient," MIT Technology Review. https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/ (accessed Mar. 31, 2021)

About the authors

Paul Cheney is a researcher working in the fields of Risk Management, Artificial Intelligence and Critical Infrastructure Security and Operations.

Ian R. McAndrew, PhD, FRAeS, is the Dean of Doctorate Programs and has been publishing for 25 years. He has been leading the Doctorate programs at Capitol Technology University since 2018 and is a frequent chair or keynote speaker at many international universities.

