Studies in Social Science Research
ISSN 2690-0793 (Print) ISSN 2690-0785 (Online)
Vol. 3, No. 2, 2022
www.scholink.org/ojs/index.php/sssr

Original Paper

A Practical Evaluation of Remote Work Issues and the SolarWinds Breach Using the ISO/IEC 27001 Cybersecurity Framework and the ISO/IEC 27002 Guidelines

Donald L. Buresh, Ph.D., J.D., LL.M.[1]

[1] Morgan State University, United States

Received: May 14, 2022 Accepted: May 23, 2022 Online Published: May 25, 2022

doi:10.22158/sssr.v3n2p75 URL: http://dx.doi.org/10.22158/sssr.v3n2p75

Abstract

This article outlines the ISO/IEC 27001 framework and the ISO/IEC 27002 guidelines, focusing on their application to two cybersecurity issues. In light of the Covid-19 pandemic, remote work has become commonplace. The factors regarding remote work have led organizations to address the cybersecurity vulnerabilities associated with the activity. ISO/IEC 27001 is one such framework that can effectively mitigate the effects of a cyber-attack. The SolarWinds breach is another example that is discussed in this article. The piece demonstrates that had SolarWinds Corp. implemented the ISO/IEC 27001 framework, the effects of the breach could have been significantly mitigated. The result is that the ISO/IEC 27001 framework is an effective mechanism for alleviating the negative consequences of a cyber-attack.

Keywords

ISO/IEC 27001 Framework, ISO/IEC 27002 Guidelines, Remote Work, SolarWinds Breach

Introduction

This article aims to discuss the ISO/IEC 27001 framework and the ISO/IEC 27002 guidelines based on the ISO/IEC 27001 framework. The piece outlines the ISO/IEC 27001 framework, followed by the ISO/IEC 27002 guidelines. The paper then addresses the security issues regarding remote work and the storage of vital information. The article then applies the ISO/IEC 27001 framework to the issues encountered when working remotely, followed by a similar exposition regarding SolarWinds and the SolarWinds breach. The essay then concludes that the ISO/IEC 27001 framework has value in a business setting because its compliance can reduce the effects of a cyber-attack.

ISO/IEC 27001 and 27002

This section discusses the ISO/IEC 27001-27002 security framework when considering remote work and information security of vital information. The essay first outlines the ISSO/IEC 27001 framework followed by the ISO/IEC 27002 guidelines. The paper observes that ISO/IEC 27002 elaborates on the security controls described in ISO/IEC 27001. The piece then talks about the security issues revolving around remote work, whereas in the next section of the paper, the thesis explains the security issues regarding the storage of vital information. The paper proceeds to observe that security controls Annex A.11.1 and Annex A.12.6 are the most critical because they are intimately related to the social engineering of human beings, the weakest link in a security system.

ISO/IEC 27001 Framework

ISO/IEC 27001 is an international standard regarding information security management. In 2005, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published the original standard jointly.[1] The standard was revised in 2013.[2] The standard describes the requirements necessary to establish, implement, maintain, and continually improve an information management system by making information assets secure.[3] There was a European update of the standard that was published in 2017.[4] After completing an audit, an organization can be certified by the International Standards Organization.

ISO/IEC 27001 certification[5] is a three-step process defined by ISO/IEC 17021[6] and ISO/IEC 27006[7]

---

[1] *ISO/IEC 27001 International Information Security Standard Published*, BRITISH STANDARDS INSTITUTION (Nov. 2, 2005), *available at* https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/

[2] Katie Bird, *New Version of ISO/IEC 27001 to Better Tackle IT Security Risks*, INTERNATIONAL STANDARDS ORGANIZATION (Oct. 2013), *available at* https://www.iso.org/news/2013/08/Ref1767.html

[3] *ISO/IEC 27001:2013 Information technology – Security Techniques – Information Security Management Systems – Requirements*, INTERNATIONAL STANDARDS ORGANIZATION (Aug. 14, 2013), *available at* https://www.iso.org/standard/54534.html

[4] BS EN ISO/IEC 27001:2017 – What Has Changed?, BRITISH STANDARDS INSTITUTION (n.d.), *available at* https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/

[5] *The ISO27001 Certification Process*, THE ISO 27000 DIRECTORY (2007), available at http://www.27000.org/ismsprocess.htm.

[6] *ISO/IEC TS 17021-2:2012 Conformity Assessment – Requirements for Bodies Providing Audit and Certification of Management Systems – Part 2: Competence Requirements for Auditing and Certification of Environmental Management Systems*, INTERNATIONAL STANDARDS ORGANIZATION (Revised 2016), *available at* https://www.iso.org/standard/59884.html

standards. The states include:

- ***Stage 1*** – A preliminary review of an organization's information security management system (ISMS) that checks for critical security documentation, Statement of Applicability (SoA), and the Risk Treatment Plan (RTP);
- ***Stage 2*** – A formal compliance audit compares the entity's ISMS against the ISO/IEC 27001 standard. The audit seeks confirmation that the ISMS is appropriately designed, implemented, and in operation. ISO/IEC Lead Auditors usually conduct the audit. Once a company passes this stage, it is fully ISO/IEC 27001 certified.
- ***Ongoing*** – This stage is concerned with follow-up reviews to ensure that the organization complies with the standard by employing periodic reassessment audits at least annually.

ISO/IEC 27001:2013 consists of ten clauses and a long annex. The following summarizes the content for the 14 annexes.

- ***Annex A.5*** – Information security policies (2 controls);
- ***Annex A.6*** – Organization of information security (7 controls);
- ***Annex A.7*** – Human resource security (6 controls);
- ***Annex A.8*** – Asset management (10 controls);
- ***Annex A.9*** – Access control (14 controls);
- ***Annex A.10*** – Cryptography (2 controls);
- ***Annex A.11*** – Physical and environmental security (15 controls);
- ***Annex A.12*** – Operations security procedures and responsibilities (14 controls);
- ***Annex A.13*** – Communications security, including information network management and information transfer (7 controls).
- ***Annex A.14*** – System acquisition, development, and maintenance (13 controls);
- ***Annex A.15*** – Supplier relationships and supplier service delivery management (5 controls);
- ***Annex A.16*** – Information security incident management and improvement (7 controls);
- ***Annex A.17*** – Information security aspects of business continuity management dealing with continuity and redundancy (4 controls); and
- ***Annex A.18*** – Compliance with legal and contractual requirements (8 controls).[8]

ISO/IEC 27002 Guidelines

For ISO/IEC 27002, the guidelines have five introductory chapters. The main chapters of ISO/IEC 27002 elaborate on the fourteen annexes in ISO/IEC 27001 framework. Each chapter contains security

[7] ISO/IEC 27006:2011 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, INTERNATIONAL STANDARDS ORGANIZATION (Revised 2015), *available at* https://www.iso.org/standard/59144.html

[8] Luke Irwin, *ISO 27001 Annex A Controls Explained*, IT GOVERNANCE (Jul. 27, 2020), *available at* https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

controls and their objectives, where the objectives are specified and outlined.[9] The information security controls are considered best practices, providing the means to achieve those objectives.[10]

Under the ISO/IEC 27002 guidelines, an organization is expected to generate an information security risk assessment before deciding on the appropriate controls, given the firm's circumstances. The risk assessment process is covered in ISO/IEC 27005.[11] It should be remembered that not all security control objectives are relevant to every organization.[12] This fact ensures that the standard is relevant in the evolving nature of information security. It is not practical to list all possible controls in a security standard. ISO/IEC 27002 lists security controls relevant to the telecommunications industry.[13]

ISO/IEC 27002 guidelines are a detailed extension of the ISO/IEC 27001 framework. The vast majority of organizations implement a wide range of information security controls, of which many are recommended by ISO/IEC 27001 and ISO/IEC 27002. It is to a firm's advantage to structure its information security controls consistent with ISO/IEC 27002 guidelines because they are internationally well respected, coverage gaps and overlaps are avoided, and a corporation's security controls will probably be recognized by individuals familiar with the ISO/IEC 27001 framework.

Security Issues Regarding Remote Work

In light of the Covid-19 pandemic, remote work is becoming highly popular and a common practice worldwide.[14] Although remote work increases flexibility for an employee, improves productivity, enhances work-life balance, and reduces employer costs, the disadvantage is that there are security risks associated with the practice.[15] Soare recommended that firms invest in a zero-trust model and identity-centric services to cope with increased cyber-attacks.[16] In particular, the five bad habits of remote workers that endanger corporate security include:

- Accessing sensitive data through unsafe wi-fi networks;
- Using personal devices for work;

---

[9] ADAM GORDON (ED.), OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK (CRC Press 2015).

[10] *Id.*

[11] *ISO/IEC 27005:2018 Information technology – Security Techniques – Information Security Risk Management*, INTERNATIONAL STANDARDS ORGANIZATION (2018), *available at* https://www.iso.org/standard/75281.html

[12] ISO/IEC 27002:2013 Information technology – Security Techniques – Code of Practice for Information Security Controls, INTERNATIONAL STANDARDS ORGANIZATION (2022), *available at* https://www.iso.org/standard/54533.html

[13] *Id.*

[14] Bianca Soare, *Most Common Remote Work Security Risks*, HEIMDAL SECURITY (Jul. 22, 2021) *available at* https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/

[15] *Id.*

[16] *Id.*

- Ignoring basic physical security practices in public places;
- Using weak passwords; and
- The practice of unencrypted file sharing.[17]

The security risks that remote working poses for companies encompass:

- Email scams;
- Security controls are weaker;
- Cyberattacks on remote-working infrastructure; and
- Threats from inside and outside an organization.[18]

When a firm permits its employees to work remotely, it must have a remote work policy. Items that should be in the policy are:

- Specify which positions are eligible for remote work;
- List the tools and platforms that remote workers should be using; and
- Provide remote employees with steps to follow at the first signs of account compromise.[19]

Some fundamental tools that remote and regular employees should use are:

- Multi-factor authentication;
- Password manager;
- Virtual private network (VPN);
- Firewalls and virus protection; and
- A robust endpoint detection and response (EDR) solution.[20]

According to OpenVPN, 90 percent of IT professionals believe that remote work is insecure, while 70 percent think remote workers are more significant than onsite employees.[21]Kaspersky Labs discovered that 73 percent of remote workers did not receive cybersecurity guidance and that 68 percent of remote workers use personal devices when working.[22] Also, 27 percent of remote workers stated that they had received phishing emails regarding Covid-19.[23] Remote work has its share of security risks. Even

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Remote Work Is the Future — But Is Your Organization Ready for It?*, OPENVPN (n.d.), *available at* https://openvpn.net/blog/remote-workforce-cybersecurity-quick-poll/

[22] *Kaspersky Research Finds 73% of Employees Have Not Received Remote Working Cybersecurity Guidance*, KASPERSKY LABS (May 7, 2020), *available at* https://usa.kaspersky.com/about/press-releases/2020_kaspersky-research-finds-73-of-employees-have-not-received-remote-working-cybersecurity-guidance

[23] *Id.*

though firms can save $11,000 per remote work annually,[24] security costs are associated with the decision. Care should be taken to mitigate the disadvantages while enjoying the benefits.

Security Issues Regarding the Storage of Vital Information

Although data protection and data privacy are considered interchangeable terms, data protection is concerned with the tools and policies that restrict access to data, whereas data privacy determines who has access to data.[25] Data protection and privacy are concerned with personal health information (PHI) and personally identifiable information (PII).[26] Data protection is vitally important in business operations and relies on data loss prevention (DLP), storage with built-in data protection, firewalls, encryption, and endpoint protection technologies.[27]

Data protection, also known as data security, is a collection of strategies to ensure data privacy, availability, and integrity.[28] A data protection strategy is critical for any entity that collects, stores, uses, disseminates, or destroys sensitive data, thus preventing data loss, theft and corruption by minimizing the damage to data from a breach or a disaster.[29] The key data protection principles are:

- ***Data availability*** – Ensuring that users can access data or use data to perform their business activities;
- ***Data lifecycle management*** – Automating the reception and transmission of critical data; and
- ***Information lifecycle management*** – Valuating, cataloging, and protecting information assets from facility outages and disruptions, application and user errors, machine failure, and malware and virus attacks.[30]

Some typical data protection practices and technologies are:

- ***Data discovery*** – Discovering what data sets exist in the organization, what data sets are business-critical, and what data sets contain sensitive data subject to compliance regulations;
- ***Data loss prevention (DLP)*** – A collection of strategies and tools that are used to prevent data from being stolen, lost, or accidentally deleted.
- ***Storage with built-in data protection*** – Modern storage equipment that possesses built-in disk clustering and redundancy.
- ***Backups*** create copies of data stored separately, ensuring that the data can be restored later in case of loss or modification.

---

[24] Remote Work Is the Future, *supra*, note 21.

[25] *Data Protection and Privacy: 12 Ways to Protect User Data*, CLOUDIAN (n.d.), *available at* https://cloudian.com/guides/data-protection/data-protection-and-privacy-12-ways-to-protect-user-data/

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

- ***Snapshots*** are complete images of a protected system, including data and system files, similar to a backup.
- ***Replication*** is a technique for copying data from a protected system to another system on an ongoing basis.
- ***Firewalls*** are utilities that monitor and filter network traffic.
- ***Authentication and authorization*** are controls that verify credentials and ensure that user privileges are applied correctly.
- ***Encryption*** is a technique that algorithmically alters data content that can only be reversed with the correct encryption key to prevent unauthorized access.
- ***Endpoint protection*** is a technique that protects gateways to a network, including ports, routers, and connected devices.
- ***Data erasure*** is a technique that limits liability by deleting data that is no longer needed.
- ***Disaster recovery*** is a set of practices and technologies that determine how an organization deals with disasters, such as cyber-attacks, natural disasters, or large-scale equipment failures.[31]

Although the list of data protection techniques is relatively extensive, it is by no means comprehensive. Other techniques exist that also protect personal information.

Two Examples of How ISO/IEC 27001 and 27002 Work in Practice

In this section, two examples are examined to demonstrate how to apply ISO/IEC 27002 and 27002. The first example discusses how the ISO/IEC 27001 and 27002 security controls can be applied when individuals work remotely. The second example shows how SolarWinds could have used the ISO/IEC 27001 framework and 27002 security guidelines to avoid and mitigate the cyber-attack it experienced.

ISO/IEC 27001 and 27002 Security Controls and Working Remotely

This section aims to decide which controls in the Annex of ISO/IEC 27001 are critical relative to remote work and the protection of vital information when present on a storage device. The relevant Annexes are Annex A.9 – Access control, Annex A.11 – Physical and environment security, Annex A.12 – Operations security procedures and responsibilities, and Annex A.13 – Communications security, including information network management and information transfer.

The aim of Annex A.9 is to warrant that employees only view information relevant to their job. This Annex is connected to social engineering, but the relationship is not strong. Annex A.11 contains 15 security controls. The security control that is the most highly correlated with social engineering is Annex A.11.1, where its objective is to prevent unauthorized physical access, damage, or interference to an entity's premises or the sensitive data held therein. Annex A.13 is concerned with how an organization protects the information in its networks. This Annex is more focused on hardware and software defenses and less directed towards social engineering issues.

When dealing with security, the weakest link is a human being.[32] In other words, social engineering is

[31] *Id.*

usually quite rewarding for cybercriminals. The Annex that involves social engineering is likely to contain the security control that is of most significant importance to an organization.[33] Based on the Annexes listed in the previous paragraph, Annex A.12 is the Annex that most closely meshes with social engineering issues.

All seven sections of Annex A.12 address social engineering in one way or another. There are the following seven sections of Annex A.12 that may deal with social engineering, including:

- ***Annex A.12.1*** addresses operational procedures and responsibilities, ensuring that the correct operations are in place;
- ***Annex A.12.2*** deals with malware, making sure that the organization has the necessary defenses to mitigate infection risk;
- ***Annex A.12.3*** covers an organization's requirements when backing up systems to prevent data loss;
- ***Annex A.12.4*** is concerned with logging and monitoring security events when they occur.
- ***Annex A.12.5*** speaks to an organization's requirements in protecting the integrity of operational software;
- ***Annex A.12.6*** encompasses technical vulnerability management, ensuring that unauthorized parties do not exploit system weaknesses; and
- ***Annex A.12.7*** addresses information systems and audit considerations by minimizing the effect that audit activities have on operation systems.

Of the seven sections of Annex A.12, Annex A.12.6 has the highest correlation with social engineering because it is concerned with unauthorized parties that may exploit system weaknesses. The whole point of social engineering is for cybercriminals (unauthorized parties) to exploit system weaknesses by exploiting human frailties. Thus, security control is the most critical implementation of the sections in Annex A.12, A.12.6.

ISO/IEC 27001 and 27002 Security Controls and the SolarWinds Cyber-Attack

This section aims to analyze the SolarWinds cyber-attack from the perspective of the ISO/IEC 27001-27002 standards. First, the SolarWinds attack is highlighted, followed by a short discussion of the ISO/IEC 27001 and ISO/IEC 27002 standards. Third, the various security controls violated by the supply chain attack are discussed. Finally, the essay concludes by saying that SolarWinds may need to review the ISO/IEC standards when attempting to improve and enhance its information security policies and practices.

SolarWinds Corp.

SolarWinds is an American software company that began in Tulsa, Oklahoma, co-founded by David

[32] *Social Engineering*, IMPERVA (n.d.), *available at* https://www.imperva.com/learn/application-security/social-engineering-attack/

[33] *Id.*

and Donald Yonce.[34] [35] The company developed the software product Orion.[36] The application supports governments and businesses in maintaining and managing their networks, systems, and information technology infrastructure.[37] The company's headquarters is in Austin, Texas, and it has over 3,300 employees across the United States and other countries.[38] [39] SolarWinds was first publicly traded in May 2009.[40] As of December 2020, SolarWinds had approximately 300,000 customers, including various federal agencies and almost all Fortune 500 companies.[41] About 33,000 public and private customers employed Orion.[42]

The SolarWinds Cyber-Attack

The SolarWinds attack began with a tiny strip of code on September 12, 2019.[43] According to

[34] Lori Hawkins, *SolarWinds Keeps on Growing*, STATESMAN NEWS NETWORK (Undated Dec. 12, 2018), *available at* https://www.statesman.com/business/employment/solarwinds-keeps-growing/JkhMoapafA0qdJvD5MFILM/

[35] Liana B. Baker, Greg Roumeliotis, *SolarWinds Confirms It Is Exploring Strategic Alternatives*, REUTERS (Oct. 9, 2015), *available at* https://www.reuters.com/article/us-solarwinds-m-a/exclusive-solarwinds-in-talks-with-buyout-firms-about-a-sale-sources-idUSKCN0S31OT20151009

[36] Saheed Oladimeji, *SolarWinds Hack Explained: Everything You Need to Know*, TECHTARGET (Jun. 16, 2021), *available at* https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[37] *Id.*

[38] Bloomberg Staff, *SolarWinds, Corp.*, BLOOMBERG (n.d.), *available at* https://www.bloomberg.com/profile/company/0OI:GR

[39] Treva Lind, *SolarWinds blows into Post Falls*, SPOKANE JOURNAL OF BUSINESS (Sep. 22, 2011), *available at* https://www.spokanejournal.com/local-news/solarwinds-blows-into-post-falls/

[40] Michael Novinson, *$286M Of SolarWinds Stock Sold Before CEO, Hack Disclosures*, THE CHANNEL CO.: CRN (Dec. 16, 2020), *available at* https://www.crn.com/news/security/-286m-of-solarwinds-stock-sold-before-ceo-hack-disclosures

[41] Catalin Cimpanu, *SEC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack*, ZDNET (Dec. 14, 2020), *available at* https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/

[42] *Id.*

[43] Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Attack*, NATIONAL PUBLIC RADIO (NPR) (Apr. 16, 2021), *available at* https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Temple-Raston, the code checked whether the computer was running a 32-bit or 64-bit processor.[44] The code returned a 0 or a 1, depending on what it found.[45] The code attempted to prove whether it could modify SolarWinds' signed-and-sealed software code.[46] Once the hackers realized they could engage in a supply chain attack, they understood that they could infiltrate Orion.[47] A supply chain attack is a hacking technique where an adversary inserts malicious code or components into a trusted software application.[48] The idea behind the attack was to compromise a single supplier so that hackers could hijack its distribution system, converting any application sold, including hardware and software, into Trojan horses.[49] With the placement of a pregnant piece of code, a hacker can infect hundreds, if not thousands, of computers as a supplier provides its wares to its customers.[50]

In February 2020, the threat actors inserted malicious code into Orion, the SolarWinds' production software, and in March 2020, SolarWinds began distributing signed software patch updates to Orion that contained the malicious code.[51] In November 2020, FireEye, a cybersecurity professional services firm, stated that it had detected a software intrusion into its systems, and on December 12, 2020, FireEye informed SolarWinds that Orion had been compromised.[52] On December 13, 2020, FireEye issued a technical analysis of the malicious software in the Orion updates.[53] On December 14, 2020, SolarWinds informed the Securities and Exchange Commission of the cyber-attack.[54] On December 15, 2020, Microsoft and its partners acted swiftly, redirecting and preventing malicious network traffic from getting to its intended destination address.[55]

On December 16, 2020, the National Security Council (NSC) staff triggered the Cyber Unified Coordination Group (UCG), which consisted of the Cybersecurity and Infrastructure Security Agency

---

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Andy Greenberg, *Hacker Lexicon: What Is a Supply Chain Attack?*, WIRED (May 31, 2021), *available at* https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/

[49] *Id.*

[50] *Id.*

[51] Vijay A. D'Souza, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, WATCHBLOG (Apr. 22, 2021), *available at* https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

[52] *Id.*

[53] Id.

[54] *Id.*

[55] *Id.*

(CISA), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) that is supported by the National Security Agency (NSA).[56] On December 18, 2020, the CISA briefed Congress about the breach.[57] On December 23, 2020, CrowdStrike, a cybersecurity professional services company, released the CrowdStrike Reporting Tool, a software application that may be employed to identify cyber risks to the Microsoft Azure Active Directory.[58] The Microsoft Azure Active Directory is a cloud-based identity and management access service that helps employees sign in and access internal and external resources.[59] On December 24, 2020, the CISA released Sparrow, a software application that can detect malicious activity for Microsoft Azure and the Microsoft Office 365 cloud environments.[60] On December 31, 2020, Microsoft reported unusual internal company accounts and unauthorized source code viewing activity.[61]

On January 5, 2021, the UCG opined that the malicious code probably originated from Russia.[62] However, at the time, President Trump hinted that the SolarWinds hack could have come from China, although no evidence was made public.[63] Even so, it should be understood that China has been involved in several high-profile hacks and could have been responsible for the attack.[64] [65]

On January 13, 2021, appointed a Deputy National Security Adviser for Cyber and Emerging Technology (DNSA-CET) was responsible for guiding the response to the breach by the federal government.[66] On February 8, 2021, the CISA released the StarBurst (AR21-039A) and TearDrop (AR21-039B) reports that analyzed the Orion malware.[67] On February 17, 2021, the DNSA-CET

---

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] Justin Hall, Kent Sharkey, Bill Anderson, & Alex Buck, *What is Azure Active Directory?*, MICROSOFT CORP. (Jun. 5, 2020), *available at* https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

[60] Vijay A. D'Souza, *supra*, note 51.

[61] *Id.*

[62] *Id.*

[63] Saheed Oladimeji, *supra*, note 36.

[64] *See generally*, CSIS Staff, *Significant Cyber Incidents*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (n.d.), *available at* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[65] Dorothy Denning, *How the Chinese Cyberthreat Has Evolved*, SCIENTIFIC AMERICAN (REPRINTED FROM THE CONVERSATION (Oct. 7, 2017), *available at* https://www.scientificamerican.com/article/how-the-chinese-cyberthreat-has-evolved/

[66] Vijay A. D'Souza, *supra*, note 51.

[67] *Id.*

stated that Russians were the likely threat actors and that the malware affected nine federal agencies.[68] On February 18, 2021, Microsoft reported that the threat actor was unsuccessful in accessing the company's code repositories in early January.[69]

On February 23, 2021, SolarWinds, Microsoft, CrowdStrike, and FireEye testified before the Senate Intelligence Committee. On February 26, 2021, the House committees on Homeland Security and Oversight and Report conducted a joint hearing regarding the SolarWinds security breach.[70] On March 10, 2021, the House Committee on Appropriations and the Homeland Security Subcommittee discussed modernizing the federal response to cybersecurity.[71] On March 18, 2021, the Senate Homeland Security and Governmental Affairs Committee held a similar hearing on understanding and responding to the attack.[72] On the same day, the CISA released its Hunt and Incident Response Program, a software tool that allows organizations to discover compromising indicators of malicious activity.[73] On April 15, 2021, the NSA, CISA, and the FBI stated that the Russian Foreign Intelligence Service (FIS) was the threat actor, and on April 19, 2021, the NSC staff deactivated the Cyber UCG, stating that the lessons learned will help to improve federal government responses to malicious attacks.[74]

Mechanisms or Policies that Should Have Existed

It was previously stated that the SolarWinds cyber-attack was a supply chain attack, where the threat actors inserted malicious code into a signed software patch top Orion, the company's software product.[75] Of utmost importance is Annex A.15 of ISO/IEC 27001 because it deals directly with supplier relationships and supplier service delivery management. In particular, Annex A.15.1concerns the protection of an organization's valuable assets that are accessible to or affected by suppliers. In the SolarWinds attack, the valuable asset would be its Orion product. The other security control that SolarWinds should have addressed was Annex A.15.2, the security control that safeguards both parties to sustain the contractually agreed level of information security and service delivery.

Annex A.8 is marginally at issue. Annex A.8.1 is concerned with identifying information assets within the scope of the company's ISMS. Although SolarWinds likely identified software assets, the value of the code protecting those assets was likely not sufficiently understood. The security control in Annex A.8.2 was probably not sufficiently defended because the supply chain attack occurred. Annex A.8.3 security control was violated because sensitive data were disclosed and possibly modified, removed, or

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] Vijay A. D'Souza, *supra*, note 51.

destroyed without authorization due to the supply chain hack.

SolarWinds violated Annex A.11.2 because the security control encompasses hardware, software, and physical files. In this instance, it is the software files that are at issue. Furthermore, there were operations security breaches. In particular, a supply chain cyber-attack is malware, and thus Annex A.12.2 was violated. By implication, Annex A.12.4 security control may have been infringed because it is concerned with the logging and monitoring of security events. Annex A.12.5 was probably affected because it deals with the integrity of operational software. Annex A.12.6 covers technical vulnerability management and is dedicated to ensuring that unauthorized individuals do not exploit a system's weakness. By definition, a supply chain cyber-attack was exploiting Orion's system weaknesses.

SolarWinds should address the damages resulting from violating security controls in Annex A.13, particularly Annex A.13.1 and Annex A.13.2. Annex A.13.1 addresses whether the confidentiality, integrity, and availability of information remain intact on a network. Annex A.13.2 is concerned with data in transit. As third-party data moved from system to system, SolarWinds' Orion was responsible for ensuring the integrity of the data. Thus, Annex A.13.2 was likely violated.

Annex A.16 is about how an organization manages and reports security incidents. This security control was likely breached if the cyber-attack was not reported promptly. Annex A.17.1 addresses information security continuity, while Annex A.17.2 examines redundancies, assuring data availability. Finally, Annex A.18 looks at the relevant laws and regulations. In the heyday of the attack, this security control was probably not followed.

In summary, there were various security controls that SolarWinds violated. The supply chain cyber-attack likely exposed multiple security vulnerabilities, particularly when the attack is viewed from the ISO/IEC 27001-27002 perspective. The number of possible infractions is directly related to the type of attack. In this instance, a supply chain attack caused many breaches of the ISO/IEC standard. The result is that SolarWinds should likely extensively review its cyber practices, keeping the ISO/IEC standard in mind.

Conclusion

In conclusion, the point of this paper was to demonstrate how to apply the ISO/IEC 27001 framework to the remote working activity, followed by how SolarWinds could have mitigated or reduced their losses had the organization implemented the ISO/IEC 27001 framework. The main idea expressed herein is that a cybersecurity framework such as ISO/IEC 27001 is an effective mechanism to reduce an entity's exposure to cyber-attacks. It should be remembered that no cybersecurity framework can eliminate the effects of a cyber-attack. What can happen is that the proper implementation of security controls can reduce the magnitude of an attack. It is the good news about cybersecurity frameworks.

Donald L. Buresh Biography

Donald L. Buresh earned his Ph.D. in engineering and technology management from Northcentral University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School). Dr. Buresh received an M.P.S. in cybersecurity policy and an M.S. in cybersecurity concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, and negotiation at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée at a local fencing club.

Miscellaneous Considerations

Author Contributions: The author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Acknowledgments: I acknowledge the insights on ISO/IEC 27001 and 27002 that I was fortunate enough to receive from Attorney Marc Roman. His comments were invaluable.

Abbreviations:

The following abbreviations are used in this manuscript:

Abbreviation	Description
CISA	Cybersecurity and Infrastructure Security Agency
DLP	Data Loss Prevention
DNSA-CET	Deputy National Security Adviser for Cyber and Emerging Technology
EDR	Endpoint Detection and Response
FBI	Federal Bureau of Investigation
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
NSA	National Security Agency
NSC	National Security Council

ODNI	Office of the Director of National Intelligence
PHI	Personal Health Information
PII	Personal Identifiable Information
RTP	Risk Treatment Plan
SoA	Statement of Applicability
UCG	Cyber Unified Coordination Group
VPN	Virtual Private Network