UNIVERSITY OF CAMBRIDGE

Cambridge Security Initiative Report

by

Nicholas Williams

A document submitted to the University of Cambridge in fulfillment of the International Security and Intelligence Programme 2023, in collaboration with King's College London, Department of War Studies

University of Cambridge, Magdalene College, Benson Court K6
Magdalene Street, Cambridge, Cambridgeshire, CB3 0AG, UK

August 2023

THIS PAGE LEFT INTENTIONALLY BLANK

Author's Declaration

The author hereby grants to Cambridge University permission to reproduce and to distribute publicly paper and electronic copies of this research document in whole or in part in any medium now known or hereafter created.

Sign and Date: _____

David Gioe, Ph.D.
Chair of the Cambridge Security Initiative

Sign and Date: _____

Tom Maguire, Ph.D.
Research Supervisor

Sign and Date: _____

Nic Williams, B.S.
Student

THIS PAGE LEFT INTENTIONALLY BLANK

Dedication

Many thanks to the Cambridge Security Intelligence Programme (CSi) for admission. Their collective research, lectures, seminars, and guest appearances shaped my appreciation and understanding of the intelligence community, reignited my passion for scholarly excellence, and provided a pathway to live abroad for a short time while completing exciting research.

Another thanks to Infoblox, Inc. who allowed me to take a month off work to complete this work, and my peers who completed my work on my behalf in my absence. They also paid my time and a portion of the cost of this trip, they care about my development and I am grateful for this.

Dedicated to my family, friends, mentors, coworkers, and partner. Without their support, excitement, interest, and input I would be unable to complete my tasks or desire to do them to begin with.

THIS PAGE LEFT INTENTIONALLY BLANK

Contents

List of Figures

List of Tables

Listings

THIS PAGE LEFT INTENTIONALLY BLANK

Part I

Overview

If any man is able to convince me and show me that I do not think or act right, I will gladly change; for I seek the truth by which no man has ever injured. But he is injured who abides in his error and ignorance.

Marcus Aurelius, Meditations

Abstract

Marcus Aurelius, at one point the single most powerful person on the planet, was described by his friends and mentors as the only person worthy of such stature. His stoicism, and desire to iteratively improve himself and the empire are part of a long story of incremental change mindsets demonstrated by many industries including: Cybersecurity, Medical, Industrial, Life Sciences, etc.

Covetousness, dishonesty, betrayal, thievery, brutality, and other harmful interactions between persons are as old as humanity itself. These problems weren't solved by moving interactions to a digital landscape. Indeed, the opposite trend occurred. Attackers being removed from directly observing the impact of actions allowed for more severe and higher frequency caustic actions.

As a society, the current paradigm cure for this is to decrease the risk of becoming a target. Does cybersecurity compliance equate to secure environments? Consensus shows no. Is that partially explained by the latency between the bleeding edge and what is 'compliant' infrastructure? The goal of this research is to answer that question.

Combining the above thought train: Strong leadership incentivizes people and industries to accept persistent gradual change; cybersecurity is an area particularly devoid of rules of engagement internationally; and to date, the best method to prevent this is driven through individual decisions. Is this inherently disjointed approach to blame for our cyber woes?

Keywords

Cybersecurity, NIST, ISO, security, framework, cyber, hack, report, breach, CSF, management, data, vulnerability, compliance, standards

Definitions

Terms

- **0-day** is a vulnerability in a system or device that has been disclosed but is not yet patched, as in, it is zero days old.
- **Attributes** a control attribute is a means of categorization that aligns ISO 27002 to industry language/standards, including: InfoSec properties, cybersecurity concepts, operational capabilities, security domains, etc.
- **Control** a security control is a measure that modifies or maintains organizational risk.
- **Exploit** is a program or piece of code designed to find and take advantage of a security flaw or vulnerability in an application or computer system.
- **Hyperscaler** Cloud Service Providers (CSPs) that allow for dynamic, real-time provisioning of infrastructure to allow for massive growth and reduction in network footprint based off demand and utilization.
- **Penetration Testing** (aka pentest) is an authorized simulated attack performed on a computer system to evaluate its security.
- **Ransomware** is a family of malware that encrypts all local user data so it is unusable/unreadable without paying for a decryption key.
- **Vulnerability** a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features, or user error.

Assumptions and Limitations

The Cambridge Security Initiative (CSi) occurs over the span of one month, at the University of Cambridge, England. It is not feasible to review an entire field's worth of sources and study in this time.

There are not formal requirements for most organizations to disclose cybersecurity breaches. All data are tainted by selection bias, there isn't a complete picture of the breaches worldwide in one place, and the incident response organizations aren't required to disclose them. Cybersecurity still employs security through obscurity in this way.

Organizations are not required to be compliant, the frameworks are voluntary, or are undertaken as a part of a business goal (selling something to the federal government). It is tough to know the inherent 'value' of compliance as there are factors of efficacy a report can't show. For example, a company can be compliant, but not have the processes in place to do things at speed. Showing you can quarantine a device, but then sticking that behind a ServiceNow ticket that goes to someone out of office means the breach happens.

Attacker and defender trends lag behind the fronts of cyber warfare. Most tactics/techniques/procedures are classified until long after the fact. The assessments on the attribution discussion are impacted by the inability to see the bleeding edge with the naked eye. Organizations with this data are financially motivated to not disclose it because doing so would lose a competitive advantage.

Lastly, undergoing compliance auditing and having great security controls in place doesn't equate to protection or prevention, if you are a big enough target an attacker will do everything they can to ensure success. Look at Stuxnet at Natanz, a completely offline facility. A company can spend millions on their cybersecurity, and lose it all from an employee willingly giving their username and password. So the breach data we have can be skewed by external and internal motivations.

Problem Statement

Cybersecurity compliance frameworks are a risk-mitigation strategy. Instead of looking at breaches as events, mathematically it's easier to look at them as a chance of happening, and then evaluate business impact. This is the selected method of cybersecurity mitigation strategy because it allows business executives to assign scores for severity, which is a part of their ongoing operational framework.

Compliance governance frameworks are also a business. They are an exam, or an audit, that involves no actual penetration testing. Their goal, like other businesses, involves retaining customers and growing the user base to sustain a coin-operated shop.

Compliance governance frameworks are an information management system, *not* algorithms for the effective delivery of cyber defense. These frameworks exist for organizations to pass exams and audits, but do not teach critical operation aspects including: succession planning, change resistance, architecture, and organizational design. They teach a decision-making system prior to breaches, and are largely ineffective on breach day.

Many organizations follow these frameworks well, and are breached regardless. Are the frameworks to blame for not being specific enough? Or are the organizations to blame for not implementing properly? If neither, are the attackers to blame, out-innovating the frameworks of protection?

Our frameworks which improve through recursion aren't sufficient, and we are to investigate why through hypotheses:

H1 The frameworks are useful, but aren't current enough. The policymakers are to blame.

H2 The frameworks are useful, regardless of latency. The organizations are to blame.

H3 The frameworks aren't useful, regardless of latency. The attackers are to blame.

Original and Final Works

0.1 Original Proposal

Below is the document originally submitted to the Cambridge Security Initiative (CSi) for evaluation of suitability for admission.

Subject Area(s)

Cyber studies and security, intelligence methodology, philosophy.

Title

Refinement of Cybersecurity Intelligence Offensive and Defensive Practices in Conflict.

Description

In the theater of modern warfare, cybersecurity is used for both attacking and guarding items from infrastructure to resources. Both benefit from increasingly cheap compute and efficient semiconductor parts, allowing for expanded automated operation for decreasing costs.

To complement this trend, data residency boundaries are expanding exponentially as imperatives to service delivery change. Together, military and nonmilitary objectives are facing exponential growth of attack surface coupled with lowering opportunity cost... creating more severe and frequent cyber incidents.

This proposed research will be to examine how cybersecurity compliance schemes advance during the bleeding-edge evolution uncovered during the conflict. Frameworks like HIPAA, NIST CSF 2.0, ISO270001, and PCI-DSS share overlap with philosophies like zero trust, genetic diversity, platform

vs. point product best-of-breed, and others. Quantifying how lessons learned through conflict are incorporated into a defensive posture will justify the iterative improvement process companies and operators align themselves to.

The proposed research will also investigate the role of cybersecurity in counterintelligence, reconnaissance, and offensive best practices. Understanding the relationship between defensive practices informing offensive innovation will more firmly link organizational risk with lack of adoption or adherence.

Ultimately, the research aims to show the delay window between cybersecurity researcher discovery and the adoption of new best practice standards by policymakers.

Relevant Work

During my employment with Palo Alto Networks, I developed expertise with NIST compliance covering SLED (State, Local, Education) customers. I custom-built a map between free and licenseable features of all our products in relation to the NIST CSF. When promoted to covering Healthcare and Critical Infrastructure, I did the same for HIPAA.

Overall, I've read through, updated documentation for, and provided feedback on some of the bigger compliance frameworks within the U.S., and will use those research and advisory skills to complete further research on how and why these systems change... and depict the inertial resistance to modernization.

0.2 Final Submission

Below is the 3500-word essay submitted to CSi as a final grade for the research completed below.

Compliance is Hard, and We Aren't Even Trying

Lorem ipsum. I am due August 15th and am being written right now.

THIS PAGE LEFT INTENTIONALLY BLANK

Part II

Literature / Industry Review

1 Industry Overview

1.1 Compliance Frameworks

2011 became a year of prominent change. Fear struck the hearts and minds of our policymakers, manufacturers, and more. Millions of dollars and tens of thousands of persons identified in breaches of Google, Northrop Grumman, Morgan Stanley, Yahoo, Symantec, Juniper, and more[1] left lawmakers distraught.

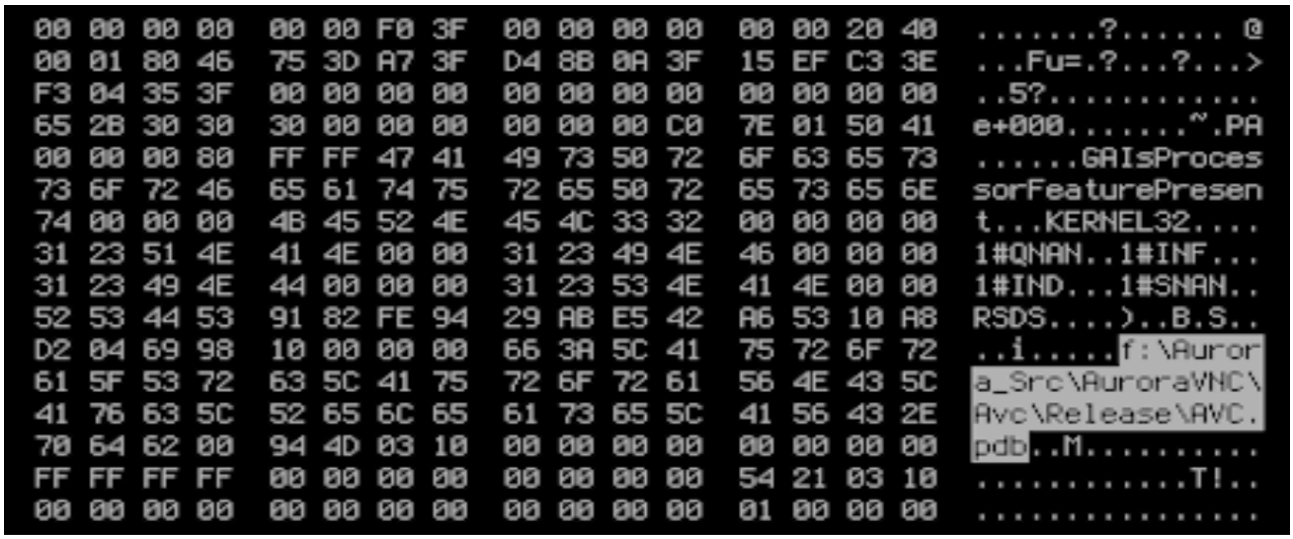


Figure 1.1: 'Aurora' malware packet capture[2]

With the attribution of major attacks increasing in volume and prominence originating from China's People's Liberation Army (PLA), the US Government needed to intervene. Beginning in February of 2013, the President signed Executive Order 13636: Improving Critical Infrastructure Cybersecurity.

[1] Varma, Rohit. "McAfee Labs: Combating Aurora." (2010).

[2] Anderson, Kevin. "US Analysis of Google Attack Code Finds Chinese Fingerprints." The Guardian, 20 Jan. 2010.

This directed the National Institute of Standards and Technology (NIST) into action to develop a framework.[3]

The order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure... the voluntary framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure.[4]

The Cybersecurity Enhancement Act of 2014 protected NIST to continue to bear this responsibility, and the Cyber and Infrastructure Security Agency (CISA) Act of 2018 elevated this mission and provided the strong backing and management of the Department of Homeland Security (DHS), resulting in the official creation of CISA.

The ongoing escalation of tensions in China over a sovereign Taiwan and their role in semiconductor manufacturing, Russian aggression and expansion into Ukraine, and other challenges abroad act as external motivators to shore up offense and defense. The US PRISM scandal following the Edward Snowden disclosures, 2022-23 Pentagon Document Leaks, and other domestic threats to operational security (OPSEC) drive desire to improve reconnaissance and behavioral analytical data at home.

For these reasons and more, in March of 2023 President Biden announces the need for a comprehensive national cybersecurity strategy[5] to drive better partnership between public and private sector operations. Companies and state organizations collect this data, below we will examine the ways they are asked to be stewards of and maintain it.

1.1.1 NIST Cybersecurity Framework (CSF)

NIST CSF 1.0 was published in February 2014 (within a year of the organization's existence), updated to 1.1 in April 2016, and is ongoing a facelift to 2.0 expected to release at any moment this summer of '23. Many updates fall into broad categories: harmonization between other frameworks, standards, and publications; added enhanced focus on supply chain security of hardware and software; added subcategories and clarified terms; and added authentication, authorization, and identity proofing

[3]Obama, Barack H. "Executive Order – Improving Critical Infrastructure Cybersecurity." National Archives and Records Administration, 12 Feb. 2013.

[4]Getting Started. NIST. (2023, April 21).

[5]"Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy." The White House, 2 Mar. 2023

sections to their protection framework.

NIST CSF 1.1 focuses on risk mitigation across 5 pillars: identify, protect, detect, respond, and recover. While many may decry this approach as not technical or encompassing enough, this framework exists as some of the most important 13 pages of cybersecurity policy nationwide and is the most accessible framework to businesses of all sizes. Many other frameworks incur large costs to utilize, bring analysts in for to validate results, and use proprietary terminology to describe concepts proving challenging for some organizations to implement. This framework trades simplicity in the hope for adoption.

While the main discussion above[6] focuses primarily on the contents within the core, other updates are coming to guidance on implementation of the core, relationship of alignment of resources between other compliance frameworks, and general interoperability with industry standards, terms, and more.

There is no formal output for being compliant to this framework, it is voluntary to participate and most popular within the United States without any requirements on disclosure of participation.

1.1.2 ISO 27001/2

There are many standards, but we will focus on 27001 and 27002. Certification in either lasts 3 years, and 270002 is typically used as a technical guide for how to implement the 270001, the eminent international framework. To begin compliance for ISO27000# services, your company would undergo a risk assessment, identify and implement security controls, and regularly measure their efficacy. To date, there are nearly 60,000 organizations worldwide certified in this standard.[7]

ISO 27001 originally published standards in October of 2005, released their first update in October of 2013, and most recently in October of 2022.[8] ISO is an *Information Security Management System* (ISMS), which isn't categorically a technical implementation document for cybersecurity practices. It is a system that focuses on vetting people, processes/policies, and technology.

This includes risk management, akin to NIST, but is also inclusive of operational goals and cyber resilience as well. Proving compliance to these standards requires analysis from firms, but these firms

[6]NIST. "Discussion Draft of the NIST Cybersecurity Framework 2.0 Core." Discussion Draft of Updates to NIST CSF 1.1 Core, Apr. 2023., p2

[7]"The ISO Survey." ISO, 22 Feb. 2023.

[8]ISO, Org. "ISO/IEC 27001 Standard – Information Security Management Systems (ISMS)." ISO, 13 Apr. 2023

aren't vetting technical controls, they are assuring there are policies in place and persons to carry them out, not necessarily testing the system in practice.

ISO 27002 was formerly known as ISO 17799 which was based on the British standard BS 7799-1.[9] ISO 27002 is a guideline for which standards should be used in evaluating effective personnel, policies, and technology. Documentation exists for features and key performance indicators (KPIs) to distinguish which solution fits in which component of the framework.

There are 93 total controls in the new version of 27002.[10] These controls are inclusive of features required to meet compliance goals including: which tools should be deployed where, which features and capabilities should be covered by the tool's functionality, and how to best use the tool in ongoing cyber security and resilience operations.

ISO compliance is conducted by certified bodies which ISO maintains and trains. Output results in a certification of compliance and is predominantly popular in international markets outside of North America. However, there are a few certifying bodies and they do not typically share their customer information.

1.1.3 SOC2

SOC 2 is developed by the AICPA (American Institute of CPA's) and defines criteria for the management of user organizations' data based on the Trust Service Criteria – The Trust Service Criteria relate to security, availability, processing integrity, confidentiality and privacy related controls.[11]

To be SOC II compliant, only the first of the above five is a requirement, the rest is a maturity and risk model discussion that each company is left to decide which allows for more flexibility.[12]

SOC I reports focus on financial impact of cybersecurity risks, challenges, and how financial reporting is impacted... not exactly focused on effective security operations.

SOC2 is growing in popularity in Northern America, especially among Cloud Service Providers (CSPs), SaaS-hosted solutions, and anything with residency ties to hyperscale environments.

---

[9] A/S, Neupart. ISO 27001 - The Standard for Information Security

[10] Edwards, Max. "ISO 27002:2022 Changes, Updates and Comparison." ISMS.Online, 1 Mar. 2022.

[11] "SOC 2 and ISAE 3000." Security and Organization Controls (SOC) UK.

[12] Irwin, Luke. "ISO 27001 VS SOC 2 Certification: What's the Difference?"

There are two primary SOC2 reports, called SOC2 Type 1 and SOC2 Type 2.

SOC2 Type 1 reflects a CPA's opinion of the standards in place in a single moment of time. It is a quick examination that controls are suitable for the data they protect, and ultimately is used to back the assertions in financial statements of organizations.

SOC2 Type 2 is the same as the above, but occurs over a period of 3 months minimum, implying a much more in-depth and realistic examination of the controls in place.

SOC2 reports are able to be conducted by any licensed CPA. SOC2 compliance output is a formal attestation which are frequently used as marketing tools to attract new customers regarding an organization's proof of security mindset.[13]

1.2 Cybersecurity Landscape

The cybersecurity landscape exists as a wild west in some contexts, where both offensive and defensive players take as much from the other as possible whenever they can to spread the other's resources thin. In other contexts, strategic breaches occur as the result of a well-executed months-long plan. Lastly, some breaches occur entirely as a result of opportunity. All are valid in the scope of this analysis.

Trending analysis from existing datapoints on breaches and investigations include: CISA, UK Cybersecurity Council, EU Infromation Council, and FBI's Internet Crime Complaints Center (IC3) Report. Private data sources include: Unit 42 Malware Report, Verizon DBIR Report, and Mandiant M-Trends Report. Academic sources include: MIT, Cybersecurity Review, and the Journal of Information and Security Applications.

Capabilities are constantly evolving, new best practices are changing, and favorite methods change constantly. There are some larger datapoints we will outline here and dig into below.

1. Malware notification sources trend toward external partnerships as the predominant primary breach alert mechanism. Per geographic region, there are trends towards internal source as notification (a hypothesis for this could indicate more effective internal alerting and analytic

[13] Step-by-Step Guide SOC 2, RiskLane, Apr. 2022.

capabilities). The causes for this are outside the scope of the research, but it can be said that most breach alerts come from watchful eyes, not effective internal teams.[14]

2. Most common target is, has been, and likely will continue to be webservers running web applications on the edge as a launching point for malware campaigns. There are more clandestine entry vectors, especially sitting as root on a router (installing telemtry on a protected vendor appliance is very tough) which is the method of choice for most APT groups.[15]

3. Compliance continues to be an emerging focus subfield within cybersecurity. The UK government, for example publishes their Breaches Survey each year since 2016. As of February 2023, the UK migrated their National Cyber Strategy under the Department for Science, Innovation, and Technology (DSIT) which is primarily researched for its applicability to small-medium businesses. These trends are followed by the work of CISA and other organizations tasked with improving nationwide cybersecurity resilience.[16]

1.2.1 Malware Trends

Consensus exists across the various malware trends reports, exploits exist as primary entry vectors followed closely by phishing.[17] This gap is narrowing, pointing to a potential future where ease-of-access of attackers (or rather, a lower cost to entry for attackers) is prioritized over development of clandestine 0-days.

Of course, there will always be places for both, but if we are trying to protect the 'average' company of 'average' resources, this means focusing on mitigating exposed resources to reduce the amount of exploitable real estate and increase awareness as much as possible.

Nearly 1-in-6 of all investigations Mandiant responded to were specifically for Log4J. Next largest included F5/Big-IP and the last included VMWare Workspace One. These 3 common vulnerabilities and exposures (CVEs) alone accounted for nearly 2 in 5 of all breaches last year.[18]

There is a high diversity of malware families utilized in ransomware, the most prevalent family is

[14] Kutscher, Jurgen. "M-Trends 2023: Cybersecurity Insights From the Frontlines." Mandiant, p7-9

[15] "2023 Data Breach Investigations Report (DBIR)." Verizon Business, p17

[16] Johns, Emma, and Maddy Ell. "Cyber Security Breaches Survey 2023." GOV.UK, 19 Apr. 2023

[17] Mandiant. "Top Trends in Cyber Security: Cyber Attacks Trends: M-Trends." Mandiant, 18 Apr. 2023, p23, "2023 Data Breach Investigations Report (DBIR)." Verizon Business, p18

[18] "2023 Data Breach Investigations Report (DBIR)." Verizon Business, p28

1-in-7 attacks (Cobalt Strike, Beacon)[19], the next-largest is 1-in-25. As we move down the top 10 list we move to single-percentile digits, which means there is a large amount of effective choices for cybercriminals to utilize.

83% of malware families continue to be effective on Windows operating systems,[20] and pointed towards servers. Most of these involved Massachusetts Institute of Technology Research and Engineering (MITRE)'s T1059 Command and Scripting Interpreter to open powershell to execute further commands.

1.2.2 Attacker Trends

The FBI Internet Crime Complaint Center (IC3), exists with great visibility into attacker trends nationwide. They receive nearly 3K complaints daily,[21] and are very effective at freezing funds that are still located internally to the US. While they aren't the frontlines of advanced persistent threats (APTs) like nation-state cybercriminals, they are able to see the trends of increasing automation and scalability of the 'least-skilled' operators.

The IC3 publish annual postmortems, and their most recent reports document the primary victims of ransomware continue to be healthcare companies.[22] Attackers pick critical infrastructure, including healthcare, because they believe the victims are most likely to pay to save lives and provide uninterrupted services to their customer base. In some cases, these organizations are federally mandated to disclose cyber breaches, and provide very detailed disaster recovery plans to prevent downtime.

The U.S. continues to be a top target across all sectors and all motivations (financial crime, espionage, etc) [24], which continues with the last 10 or so years. Interestingly, they are tracking nearly 200K "subjects" across the US, which are defined as the perpetrators of the scam(s)[25]. Even if we assume a high error rate in this count (many attacks attributed to the same person incorrectly shown as multiple), this could be nearly a half a percentage point of people within the U.S. are cybercriminals. Hundreds or tens of thousands of persons.

---

[19] Mandiant. "Top Trends in Cyber Security: Cyber Attacks Trends: M-Trends." Mandiant, 18 Apr. 2023,, p38
[20] Mandiant. "Top Trends in Cyber Security: Cyber Attacks Trends: M-Trends." Mandiant, 18 Apr. 2023,, p41
[21] 2022 INTERNET Crime Report - Internet Crime Complaint Center (IC3), p17.
[22] "2022 INTERNET Crime Report - Internet Crime Complaint Center (IC3)." IC3 2022 Internet Crime Report, p14
[23] "2022 INTERNET Crime Report - Internet Crime Complaint Center (IC3)." IC3 2022 Internet Crime Report,, p19
[24] Mandiant. "Top Trends in Cyber Security: Cyber Attacks Trends: M-Trends." Mandiant, 18 Apr. 2023,, p6-10
[25] "2022 INTERNET Crime Report - Internet Crime Complaint Center (IC3)." IC3 2022 Internet Crime Report, p27

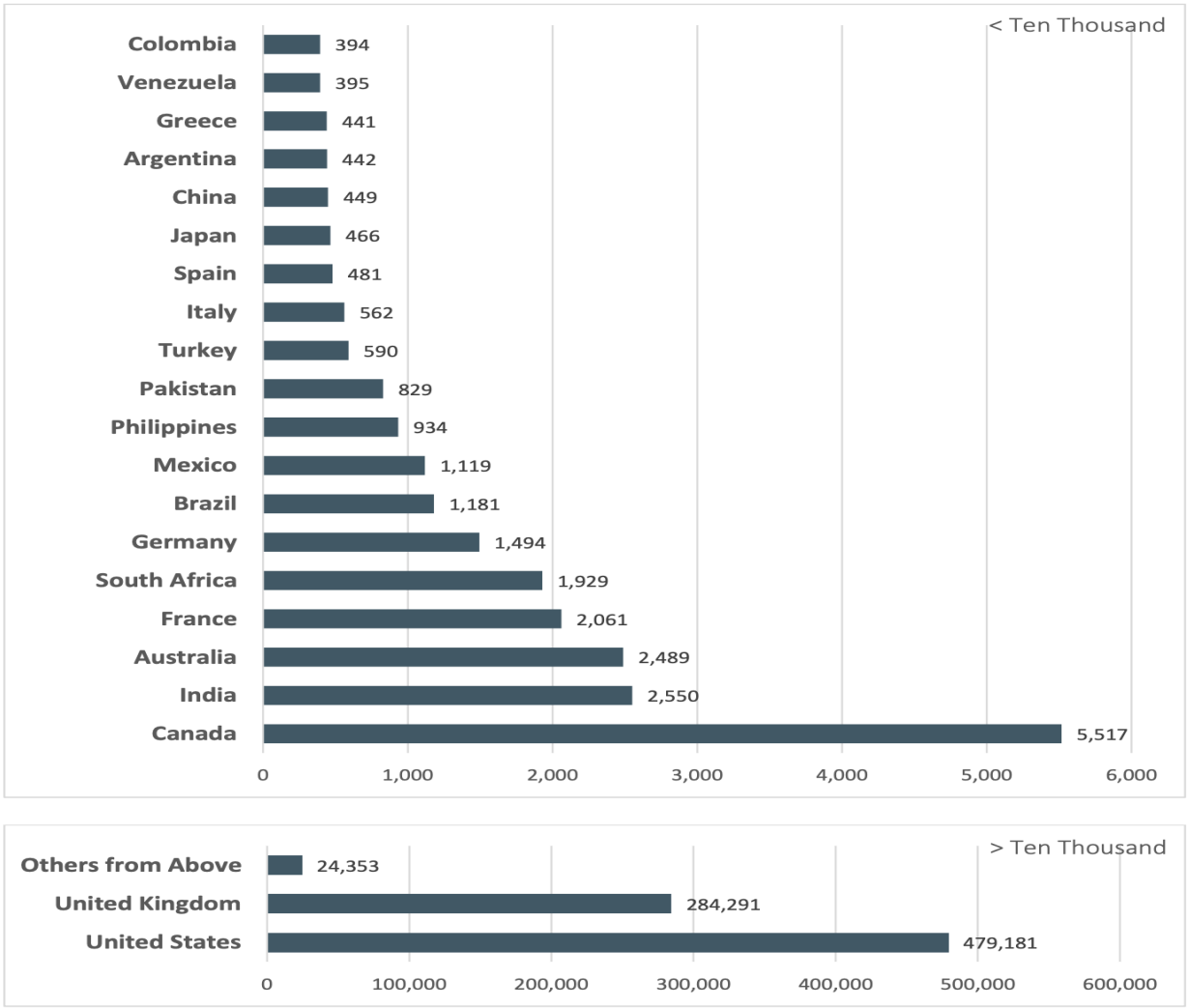


Figure 1.2: Top victim countries by source.[23]

The overwhelming majority of worldwide cybercrime is attributed to financial motivations,[26] with a notable uptick in data theft to grease the negotiation wheels.[27] Attackers are also engaging in targeted harassment of C-Suite personnel, leaking to the media, 20-fold growth.[28] Attackers utilize these approaches because unauthorized data disclosure frequently works for coercion, cold backups and disaster recovery (DR) plans don't prevent loss of reputation and confidence, and potential fines/sanctions. There have been examples of ransom going unpaid, and the targeted harassment campaigns so intense the costs to rectify exceed the ransom.[29]

[26]"2023 Data Breach Investigations Report (DBIR)." Verizon Business, p70
[27]Mar 21, 2023. "2023 Unit 42 Ransomware and Extortion Report." Palo Alto Networks, p10
[28]Mar 21, 2023. "2023 Unit 42 Ransomware and Extortion Report." Palo Alto Networks, p11
[29]Mar 21, 2023. "2023 Unit 42 Ransomware and Extortion Report." Palo Alto Networks, p12

There are additional challenges with ransomware, especially if the criminal group lives in an OFAC-sanctioned country, which can eliminate the capability to pay a ransom, in some cases. The operational capabilities of threat actor groups are expanding. In one report, LockBit ransomware group posted 801 breached organization names, compared to 409 in 2021.[30] While median and mean ransom payments are decreasing, the frequency of payments is increasing due to operational scaling.

1.2.3 Defender Trends

There are common threads across actions defenders are taking worldwide. These frameworks update largely to account for ongoing requirements to integrate optional and legal requirements from internal and external bodies per organization. The tools they utilize are increasingly evaluated for their capabilities in their regards to interoperate, and organizations struggle at large to recruit and retain skilled cyber operators.

The diversity of the medical field exists to address the explosive growth of disease diagnosis due to ongoing medical research, and provides the best avenues for delivery of breakthrough intervention options. Cybersecurity is undergoing the same challenge with none of the historical infrastructure older institutions experience.

Tools/Tactics Starting in 2021, the US Department of Defense (DoD) started recommending protective domain name system (DNS) services as part of their defense in depth strategy.[31] The trend of adding analysis capabilities inline to many transport streams is growing.

These analysis vectors are critical because they lower the 'noise' in network defense. Defenders used to forward logs and manually review them... a labor-intensive endeavor that is now impossible due to the scale of logging in the infrastructure. Below is an example of raw syslog, of which there could be millions per second in a larger network.

```
Jul 25 16:23:07 LAYER8 172.24.120.20 dhcpd: Option 82: received a REQUEST
DHCP packet from relay-agent 66.129.225.35 with a circuit-id of "52:6f:6f:74"
for 172.24.236.250 (55:4e:ee:fe:ff:ff) lease time is undefined seconds.
```

Figure 1.3: Raw Syslogs

[30] Mar 21, 2023. "2023 Unit 42 Ransomware and Extortion Report." Palo Alto Networks, p15

[31] "Selecting a Protective DNS Service - U.S. Department of Defense." Cyber Security Information, CISA, May 2021.

After this, the industry evolved to correlation rules. Regular expression (RegEx) and other pattern-matching tools allowed for the identification of anomalous traffic. However, it's inflexible and imperfect... resulting in a high amount of false positives, and worse yet – false negatives.

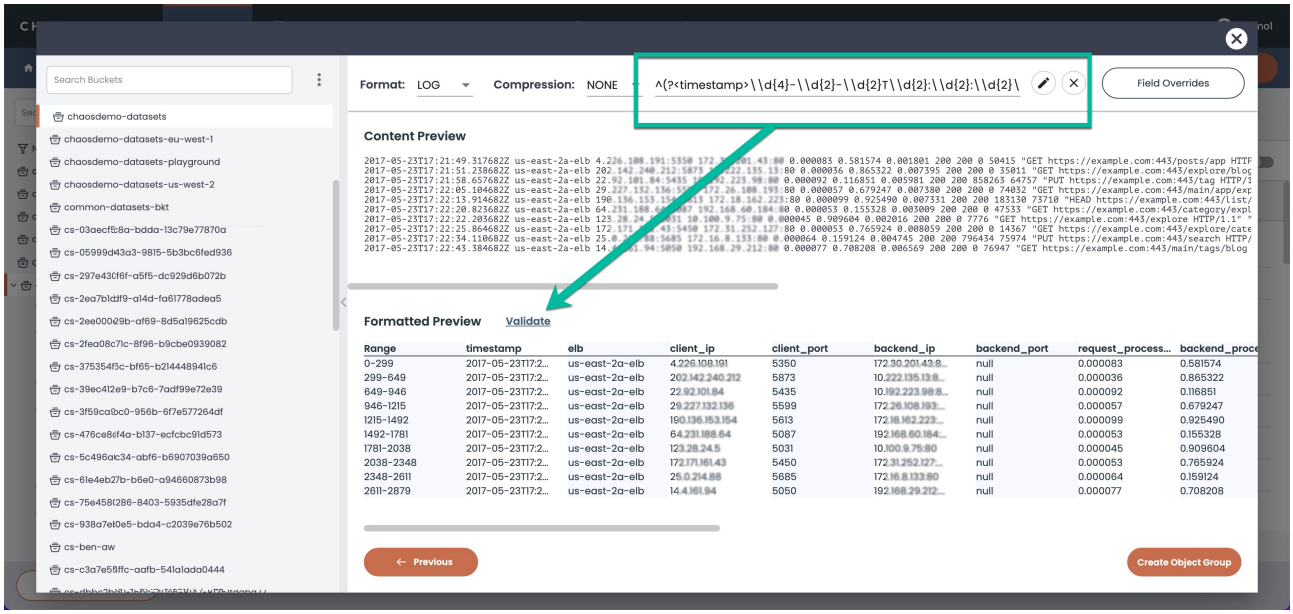


Figure 1.4: RegEx Pattern Matching Example[32]

Queries per appliance, time block, responses, protocols, locations, and many more prove too cumbersome for most organizations to use at scale, and queries against volumes of data with regularity incurs cost. Look at the below query in RegEx to better understand how many queries you would run against your logs to need to understand trending data, as this returns just IPs. How many do we need to understanding trending data compared to a timeframe?

```
/^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01
]?[0-9][0-9]?)\$/
```

Figure 1.5: RegEx to filter by IP address

Machine Learning (ML) now allows for the previous ruleset's strengths (correlation), with none of the weakness (inflexible) by iterating to better identification patterns. Furthermore, it is much more legible.

[32]"Regex Support." CHAOSSEARCH Knowledge Center.

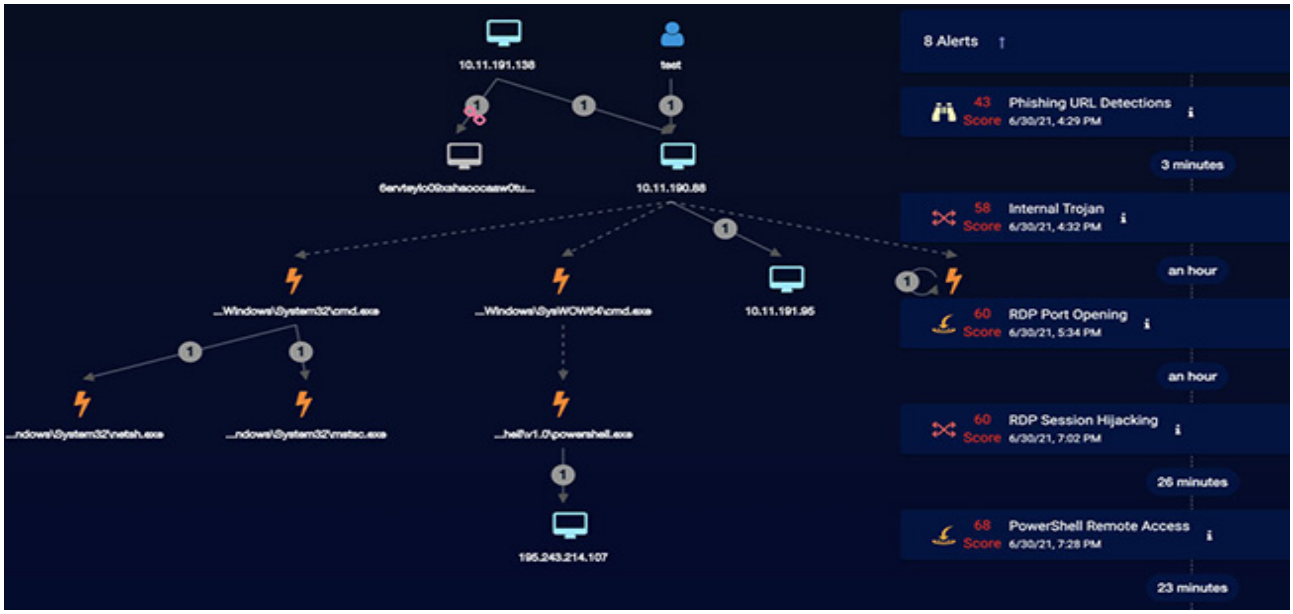


Figure 1.6: ML-powered correlation[33]

The new ML-imbued analysis tasks allow for types of comparison the previous iterations do not. For example, would a complicated RegEx pattern allow for comparative analysis between historical data? Would one query show you how traffic of a single device now is compared to a month prior?

This allows defenders to get closer to identifying anomalous *behavior* compared to peer devices, peer networks, peer organizations, and more types of comparative tooling than ever before. Many analysts attribute these types of advances as partially responsible for the decreasing detection and response times. The more rich contextual data coming from more sources, analyzed against known good data will continue to drive better security operations.

Techniques Automation frameworks, using Ansible, Terraform, and other popular templating languages allow for task replication at scale. Investigations, remediation, re-deployment, and modifying current operations are 10x faster with the right security/network operations teams (SecOps, NetOps) with some formal training in automation, scripting, programming, and more.

For mature Security Operations Centers (SOCs) monitoring their organization's assets in real-time, the industry is standardizing around technology known as SOAR: Security Orchestration Automation Response engines. These engines are clickable, programmable, user-friendly interfaces that use application programming interface (API) hooks into various products (and custom scripting calls) to

[33]"Stellar Cyber's AI-Driven Incident Correlation Increases Attack Detection Efficiency." Help Net Security.

bring all the above analysis into techniques for investigation and remediation.

These tools are expensive to purchase, operate, and maintain. It takes a skilled team to use them, and retaining and training this team is effort-intensive. The benefits are huge, however, as the scale of what is able to be investigated, remediated, and the speed of doing so decreases exponentially.

This will allow for small teams, handfuls of persons, to monitor companies of tens of thousands. Due to the natural scarcity of skilled analysts, there are some companies that offer managed services to smaller businesses to outsource the expertise they need. These managed security service providers (MSSPs) are one way the industry is consolidating resources to improve overall security posture.

However, with SOAR playbooks and analysts, now incidents are starting to be auto-triaged, and the first few steps of an incident (creating isolation, querying logs, etc) goes from a manual process to automated, leaving only decision making to the human operators. Below is an example where an analyst may see malicious logs coming from a potentially infected device, and the playbook will automatically run to isolate it, and an analyst may revisit this playbook in the future after they've replaced/repaired the hacked device.

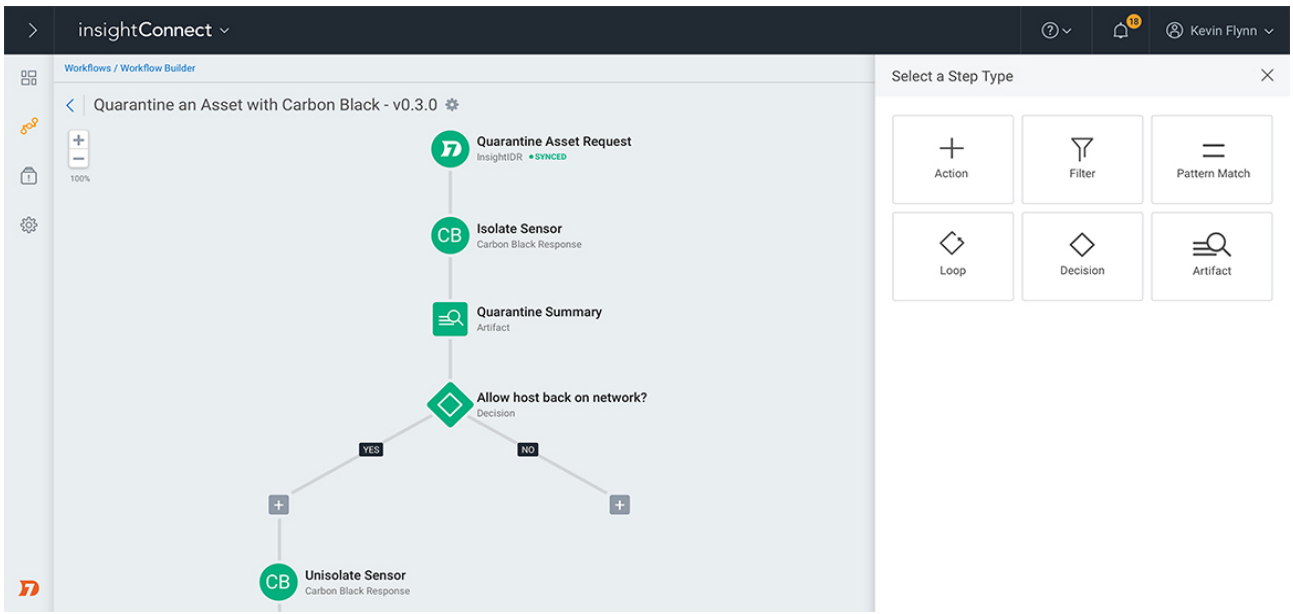


Figure 1.7: Security Orchestration Automation Response (SOAR) playbook[34]

[34] "Security Orchestration Automation and Response (SOAR) Playbook." Rapid7.

Procedures Focusing entirely on adversary detection and elimination of threats alone is not sufficient. There are companies with the most mature security programs and best-practice networks that still fall to vulnerabilities. There are no perfectly secure systems in practice (and rarely in design). To assist in risk mitigation, many cybersecurity practitioners employ the use of cyber insurance which is at best inconclusive in improving security posture.[35]

Despite the above investments in analysis technologies, and personnel to maintain them, research suggests[36] that no matter the amount of investment, organizations will continue to fall victim. Part of the improvement strategy is to create internal security cultures, awareness, and processes distributed throughout an organization. There is no question in the efficacy of cybersecurity internal audits[37], however, many corporations do not possess the teams in-house nor the funding to partake externally.

1.3 Summary

Security is becoming more effective, interconnected, and agile in the face of increasingly proficient attackers. Compliance is one of many attempts to shift the momentum of the conflict to be an advantage for defenders, which today is on the other side.

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	**2022**
Combined	416	243	229	205	146	99	101	78	56	24	21	**16**
External	–	–	–	–	320	107	186	184	141	73	28	**19**
Internal	–	–	–	–	58	80	57.5	50.5	30	12	18	**13**

Table 1.1: Global median dwell time of malware.
[38]

Governments are slow to regulate the industry, mandate changes, and the right incentives aren't in place today to ensure businesses operate in good faith in receiving their certifications and undergoing

[35]R. Pal, L. Golubchik, K. Psounis and P. Hui, "Will cyber-insurance improve network security? A market analysis," IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2014, p235

[36]Mohammed Alqahtani and Robin Braun (2021), "Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review", Journal of Information Assurance & Cybersecurity, Vol. 2021 (2021)

[37]Sergeja Slapničar, Tina Vuko, Marko Čular, Matej Drašček, Effectiveness of cybersecurity audit, International Journal of Accounting Information Systems, Volume 44, 2022

[38]Mandiant. "Top Trends in Cyber Security: Cyber Attacks Trends: M-Trends." Mandiant, 18 Apr. 2023,, p10

their audits. At the same time, governments will at times request the assistance of private sector input for policy creation, which is to limited success.

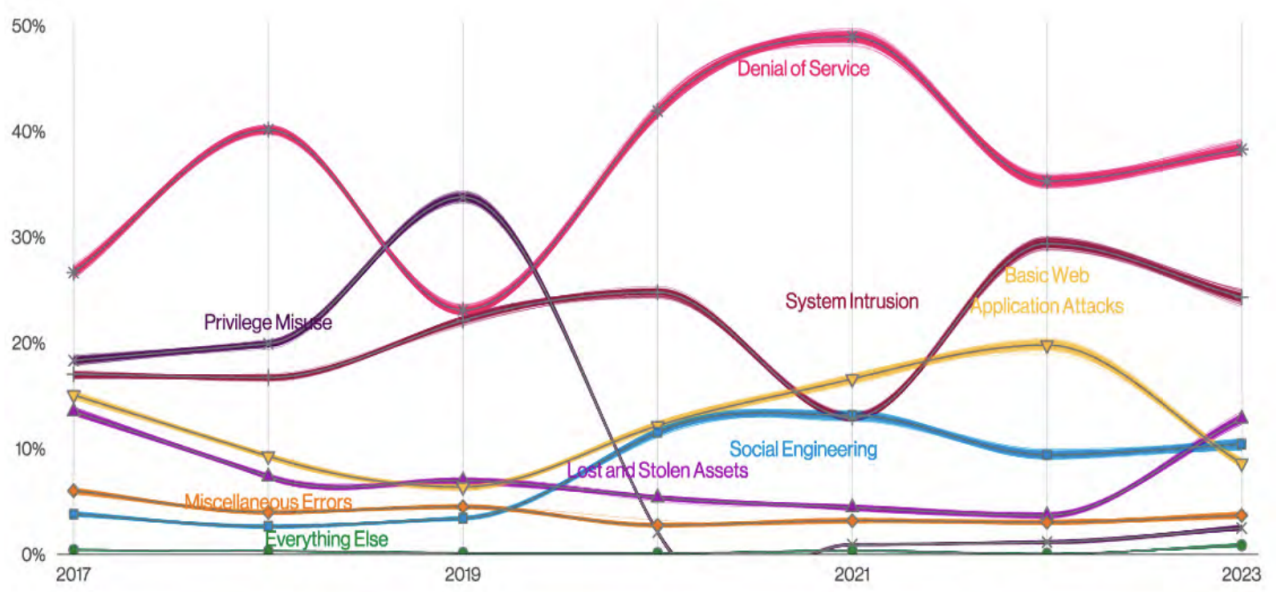


Figure 1.8: Attack types by volume[39]

On the other side, attackers are increasingly incentivized to automate their operations to easily allow break-ins to the least secure organizations. They are incentivized to collaborate and share profits, emulate techniques, and evolve their campaigns.

Lastly, awareness and education of the general public and executives is lacking in how cybercriminals operate, their goals, and outcomes. If all the above stays true, then defenders will continue to lose.

Attackers are incentivized to share data, collaborate during attacks, and private sector vendors are not. This points to ***H3*** being a likely conclusion.

[39]"2023 Data Breach Investigations Report (DBIR)." Verizon Business, p22

2 Literature Overview

2.1 Academic Sources

Print

Intel Case Study from Northeastern University, Adenekan Dedeke investigates the relationship (and limitations) between compliance-based and risk-based cybersecurity, through the lens of the implementation journey and outcomes of Intel.

Cyber Warfare Conflict Analysis and Case Studies from Gazula at MIT maps well-known cyber conflicts to a historical CASCON scale to measure impact and categorize attacks for future study.

Analysis of Factors of NIST Adoption in Financial Sector Simonova et al researched the fundamental relationship between expectations of performance, effort, and social pressures and adoption of the frameworks in financial sector.

Incentivizing Cybersecurity Compliance in the New Digital Age Modesti et al in Cardozo Law Journal establishes on legal arguments for mandating cyber breaches as injury and Congress' requirements to define and regulate these issues.

Research

Internal Audit Efficacy Research from Slapnivcar et al a study across a few hundred organizations and ISACA chapters worldwide to make a quantitative relationship of internal auditing to cybersecurity efficacy.

Examining the Impact of Technical Controls... and Compliance in Government Organizations Alqahtani et al from University of Sydney measures the efficacy of monitoring tools on employee cybersecurity behavior.

GOV.UK Cybersecurity Council Breach Report 2023 The UK councils responsible for nationwide cybersecurity provide annual reports on the country's cybersecurity state, what causes breaches, and what resources are still required to remediate them.

2.2 Industry Reports

Unit 42 Ransomware Trends from firewall vendor Palo Alto Networks, focusing on the impact and behavior of ransomware gangs.

Mandiant Malware Trends from incident response and threat intelligence service Mandiant, on worldwide trends of malware, attackers, and the state of the industry.

Verizon Data Breach Investigation Report from Verizon's business unit, a report denoting the types of attacks seen across their internet service provider (ISP) backbone.

2.3 Other

NIST Known Exploited Vulnerabilities Database, CSF 1.0/1.1/2.0

MITRE ATT&CK Framework

United States National Cybersecurity Strategy Implementation Guide

THIS PAGE LEFT INTENTIONALLY BLANK

Part III

Research

3 Methods & Dataset

The theory of this paper is to identify and correlate multiple distinct issues.

1. Popular cybersecurity frameworks, latency of each.
2. Popular exploited vulnerabilities.
3. Victim companies and their compliance status.
4. Compare the changes to each framework to vulnerabilities.
5. Compare the breached companies to frameworks.
6. Conclude on efficacy of frameworks for companies.

Items 1, 2, 4, and 5 are (mostly) public data. However, due to 3 not being public, this study will be heavily reliant on case studies (since item 5 is case-by-case basis). Without 3 and some of 5, there is no quantitative analysis at scale, therefore item 6 is a less meaningful judgment. More on this will be discussed during the conclusion.

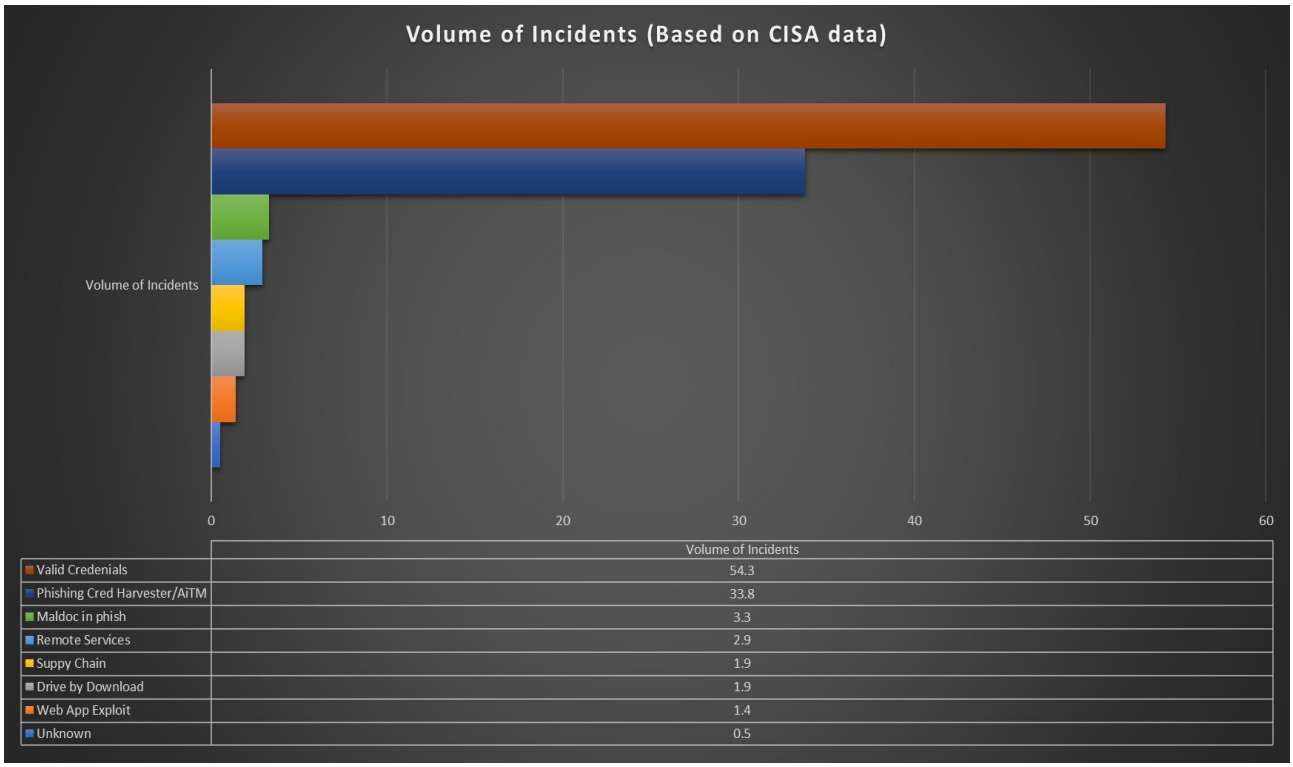
This data will be increasing in availability due to oversight changes, including the SEC passing new rules 26 July 2023[1] that public companies must disclose 'material' cybersecurity incidents within 4 days (unless national security or public health is impacted in doing so) and annual reports on cybersecurity risk mitigation strategies for investors.

While this won't affect private companies, it is a start in removing the veil obscuring this data.

[1] "Press Release." Security and Exchange Commission (SEC), 26 July 2023.

4 Cybersecurity Industry Context

While it is not possible to exhaustively document the progression of cybersecurity attacks and their consequences, there will be a few case studies described below. These case studies contrast the differences in motivations, outcomes, and even the entry vectors of attackers to show the amount of variability possible in attacks and threat vectors compared to average threats. These case studies will differ slightly from the industry trends above, remember, most attacks are to vulnerable webservers and CISA document the largest threat to most organizations are no MFA and reused credentials:



	Volume of Incidents
Valid Credenials	54.3
Phishing Cred Harvester/AiTM	33.8
Maldoc in phish	3.3
Remote Services	2.9
Suppy Chain	1.9
Drive by Download	1.9
Web App Exploit	1.4
Unknown	0.5

Figure 4.1: CISA's top threats to organizations.[1]

4.1 Significant Cybersecurity Incidents

4.1.1 Operation Olympic Games/ STUXNET

Figure 4.2: Iran's Natanz Nuclear Facility[2]

An example of action on a strategic objective and likely the most prominent example of offensive cyberattacks, STUXNET is attributed to NSO / Alphabet Group (IL / US military) to take Iran's Natanz nuclear enrichment facility offline in 2010. One of the first public-displayed uses of military cyber warfare, this attack utilized an unprecedented 5 0-day chain of exploits to gain access to programmable logic controllers (PLCs) of the centrifuges, make them spin faster, and report back to the monitoring tools nominal status. This is a clandestine, novel approach to covert action in which the objective is completed, without attribution or immediate alarm.

All the centrifuges burn up, and no longer be within operational specification. This attack took years of planning, and the facility impressively is not connected to the internet, requiring a unique delivery mechanism through offline portable media devices.

[1] "FY22 Risk and Vulnerability Assessments (RVA) Results - CISA." CISA Risk Vulnerability Assessment Center, July 2023.

[2] Ackerman, Spencer. "5 Nuclear Sites That Could Launch War with Iran." Wired, 21 May 2012.

4.1.2 ETERNALBLUE/ WANNACRY

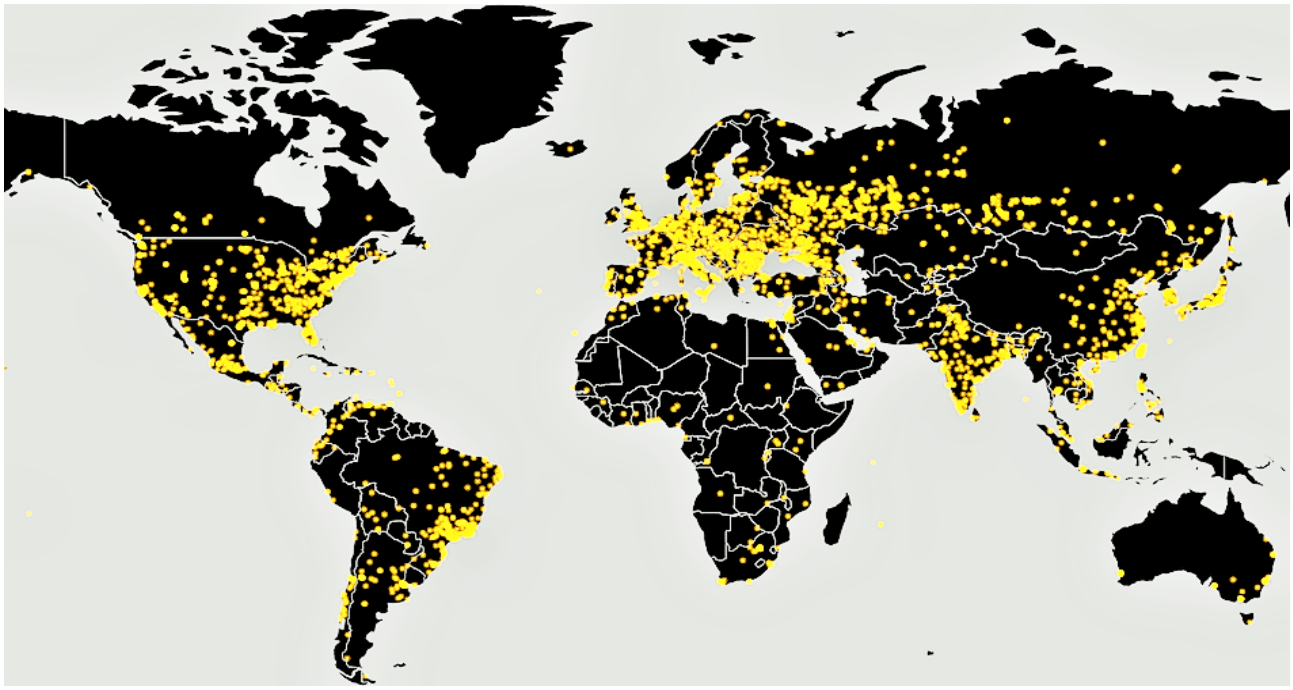


Figure 4.3: WannaCrypt0r Heatmap[3]

An example of the costs associated with developing cyber weapons, and the speed at which innovation and opportunity aid attackers. A group known as the 'Shadow Brokers' leaked exploits developed by 'The Alphabet Group' at the end of 2016 (widely associated to be the National Security Agency (NSA)), one of which is codenamed EternalBlue. EternalBlue turned out to be particularly nasty because it allowed for remote code execution on any Windows machine running server message block (SMB) protocol (all of them, essentially).

With North Korean cybercriminals attaching the ransomware family WannaCrypt0r to the exploit, they successfully spread one of the most costly cybersecurity breaches in human history. Including shutting down Maersk, the UK's NHS, and hundreds of companies worldwide, some of which never recovered. A total of nearly 300K devices were impacted across 150 countries, deployed in less than 2 months after the Shadow Brokers leak.

[3]Gupta, Amartya. "Ransomware Attack – A Nightmare for Any IT Team." Motadata, 16 May 2017.

4.1.3 MELTDOWN/ SPECTRE

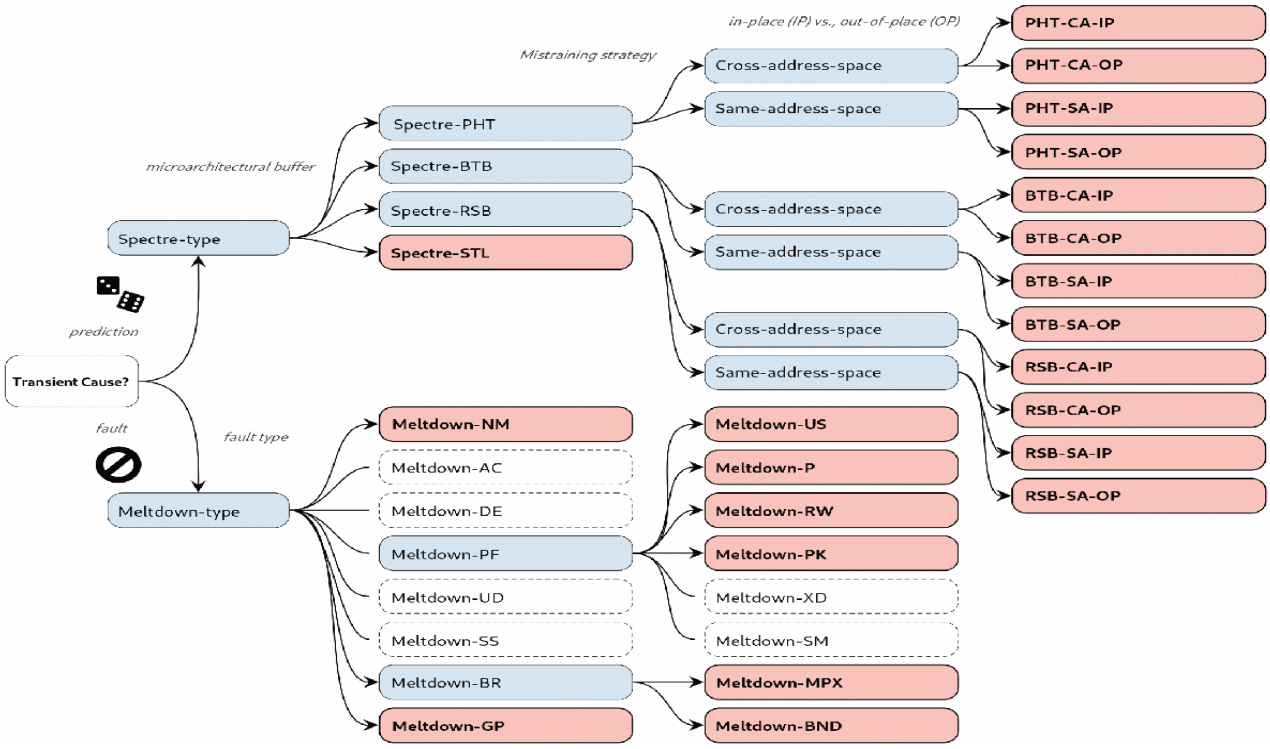


Figure 4.4: Attacks related to Spectre and Meltdown.[4]

An example of hardware vulnerabilities, which are very difficult to patch and detect. This includes ARM, Intel, IBM chipsets for all computers, laptops, and mobile devices. Essentially, most every device in operation today. Originally disclosed in 2017 to hardware vendors, it is not fully patched or mitigated years later.

While the focus of most threat actor groups occurs in software, as that is the biggest 'base' you can cover to try to attract most victims and be the most efficient in money-making operations... an attack using this family of breaches would be near-impossible to prevent or detect against.

While cybersecurity and computer manufacturing companies have yet to publish known hacks or exploits with a root cause associated with these types of threat vectors, it is important to note these are the exact types of things nation-states will sit on (EternalBlue) for a particularly high-powered operation, like StuxNet. While we haven't seen it yet, that doesn't mean we will not.

[4]Sanders, James. "Spectre and Meltdown Explained: A Comprehensive Guide for Professionals." TechRepublic, 15 May 2019.

4.1.4 HAFNIUM Exchange

Figure 4.5: APT40/HAFNIUM Group Members[5]

This attack is an example of sly espionage, HAFNIUM is an advanced persistent threat (APT) group attributed to The People's Republic of China (PRC) intelligence. In January of 2021, a group disclosed vulnerabilities to Microsoft documenting the ability for Exchange servers (normally attached to the internet directly, they run a company's email) to be remotely breached, and backdoors installed.

These backdoors were used to spy on, and exfiltrate data from defense contractors for air and ship designs to aid the PRC's naval building efforts and defense capabilities. They were ultimately successful, to the point that Microsoft now fully recommends customers no longer use physical exchange servers and is actively migrating their on-prem customers to cloud-hosted exchange.

Microsoft rushed out a patch in April to mitigate the efficacy of these attacks, but at this time hundreds of organizations already experienced backdoors within their environments. In many cases, there were successful data exfiltration from the nearly 30K rooted devices painfully showing the power of automated attacks.

[5]Corfield, Gareth. "UK and Chums Call Out Chinese MSS for Hafnium Microsoft Exchange Server Attacks." The Register, 19 July 2021.

4.1.5 SOLARSTORM / SOLARBURST

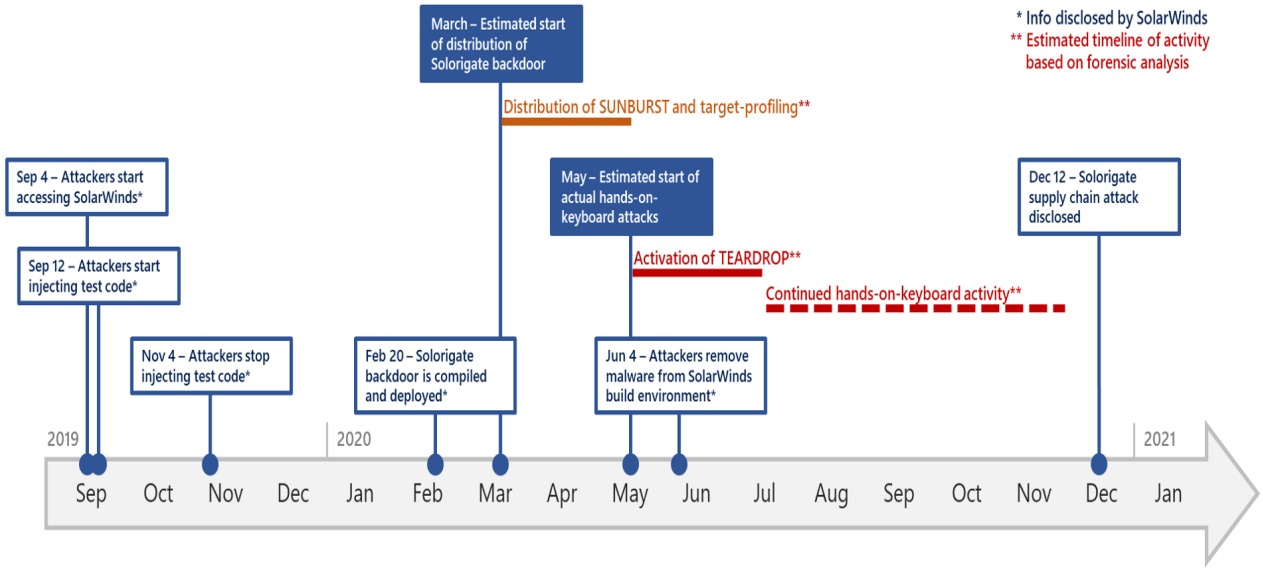


Figure 4.6: SolarWinds postmortem timeline of supply chain compromise.[6]

The most prominent example of a supply-chain attack. NOBELIUM, attributed to Russian intelligence, operated secretively within SolarWinds' production environment for months prior to acting on their objective.

SolarWinds is a high-value target, as SolarWinds tools are frequently used as logging aggregators, configuration managers, device inventory maintainers, and more. Wide deployments across public and private sector environments, they've been an industry leader in their respective space for some time. NOBELIUM used their access to SolarWinds' development environment to push test code.

Once the test code deployed successfully, they rapidly placed their malicious code within the stack. This code beaconed out to their command and control (C2) servers, and downloaded their custom Cobalt Strike droppers to execute code from within the SolarWinds appliance. Many companies were unable to detect this, as there are not ways to install monitoring software within vendor appliances.

Known exploited companies include: Intel, Cisco, FireEye, SAP, Belkin, and Deloitte[7]. While they all maintain there is no evidence of impact to their products, it is also hard to exhaustively prove no proprietary data ended up stolen.

[6]Microsoft Cyber Defense Operations Center (CDOC), Microsoft Threat Intelligence. "Deep Dive Into the Solorigate Second-Stage Activation: From SunBurst to Teardrop and Raindrop." Microsoft Security Blog, 20 Jan. 2021.

[7]Viggiani, Fabio. "The Solarwinds Orion Sunburst Supply-Chain Attack." Truesec, 16 Dec. 2020.

5 Cybersecurity Framework Latency

5.1 NIST CSF

Assessment

NIST Version	Created	Latency (Days)	US Adoption
1.0	12 FEB 2014	–	–
1.1	16 APR 2018	1,534	30%[1]
2.0	– AUG 2023	1,930+[2]	50%[3]

Table 5.1: NIST CSF version ages.

Description

NIST-compliant companies appear to be a large swath of guesses, which are all from surveys of varying sizes of IT personnel which are then extrapolated to the rest of the US population size. It is unreliable to assume a majority of companies are using the framework in a way that is meaningful, but anecdotally many are aware and working towards it.

Being that there aren't implications of punishment for lack of adoption, it isn't always the most pressing items for IT teams to commit resources to, compared to other projects like cloud migration, remote workforce integration, and scaling of operations of internal and external services.

[1] "Cybersecurity Trends: Looking Over the Horizon." McKinsey & Company, 10 Mar. 2022.
[2] As of 29 July 2023.
[3] Banga, Gaurav. "Council Post: How to Ensure Your NIST Cybersecurity Framework Implementation Isn't Too Little, Too Late." Forbes, 3 Nov. 2020.

5.2 ISO27001

Assessment

ISO Version	Created	Latency (Days)	Certified Organizations
2005	15 OCT	–	–
2013	31 OCT	2,938	43,682[4]
2022	25 OCT	3,281	58,423[5]

Table 5.2: ISO 27001 version ages.

Current 2013-compliant companies have until November 2025 to transition to the new standards before losing their current certification. Many are currently undergoing their 'gap analysis' to identify current shortcomings of controls and mitigations in place compared to the new framework definitions.

Description

The ISO survey shows good scale and growth, but, worth noting the huge majority of those customers are federal and Fortune companies. Many estimate hundreds of millions of companies exist worldwide, all combined frameworks are adopted by a thousandth of a single percentage point of companies worldwide are adopting and using this framework.

It is worth mentioning the above to point out that although frameworks are used by most large companies, the struggle with cybersecurity will continue to be one of lacking resources across smaller verticals, as adoption is both unrealistic and unprovable in many circumstances.

ISO still remains the international standard, the most adopted, widest used, and is likely the largest growing. Case studies below will demonstrate many companies and organizations fully compliant to these standards still woefully and inadequately prepared for a skilled adversary.

[4] "The ISO Survey." ISO, 27 Feb. 2013.
[5] "The ISO Survey." ISO, 22 Feb. 2023.

5.3 SOC2

Assessment

SOC Version	Created	Latency (Days)
2010	15 APR	–
2017	1 DEC	2,787
2022	15 OCT	1,779

Table 5.3: SOC version ages.

Description

SOC2 reports are available under NDA. It's the industry standard for SaaS-based tooling, so there are thousands undergoing their audits for this purpose, but it is not data accessible to the public.

5.4 Summary

Assessment

Framework	Average Latency (Days)
NIST CSF	1,732[6]
ISO27001	3,110
SOC2	2,283
Mean Average	**2,375**

Table 5.4: Average framework latency.

Description

This average equates to 6.5 years average between updates of frameworks. With published CVEs nearly daily, it will be hard to attribute specific additions to framework changes a single event. This evidence supports ***H1*** as cause for adversary efficacy.

[5]As of 29 July 2023.

6 Threat Vectors

6.1 CISA Known Exploited Vulnerabilities Database

The average organization employs over 70 tools as part of its cybersecurity stack.[1] The CVEs represented above include both vendor-specific CVEs (SolarWinds, etc), but also free open-source software (aka FOSS; OpenSSL, Linux, etc). While it may seem 173 vendors is quite small, given the prevalence of FOSS within enterprise products, it necessarily *guarantees* one will work in your environment, somewhere. Especially knowing the vendors included this list (Microsoft, Apple, Cisco, etc) fulfill core needs of businesses worldwide and are likely all present.

Created	Update Frequency	# of Entries	# of Vendors Included	# of All Known CVEs
3 NOV 2021[2]	Daily	976[3]	173	221,264

Table 6.1: CISA Known Used CVEs.

NIST's National Vulnerability Database (NVD) tracks CVE submissions worldwide, and the database sits over 200K entries today. 16K of which are from this year.[4] This means less than .5% of known CVEs are in use throughout the year, which speaks both to the size of attack surface, and speed of deployment (10%+ new disclosures year-over-year).

Few industries see this type of explosive growth, and the ones that do usually aren't tracking trending data in this capacity. For example, the medical industry continues to specialize as potential diagnoses and interventions continues to grow through research and study. The industry experiences strain and

[1] "Panaseer 2022 Security Leaders Peer Report." Panaseer, 11 July 2023.
[2] "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities: CISA."
[3] As of 29 July 2023.
[4] "Known CVE Database Dashboard." NVD - NIST.

complaints from patients due to the time it takes to get referred out to more personnel for 'simple' things.

The cybersecurity industry is experiencing 10%+ growth each year in the 'diagnosis' problems, and the number of tools/vendors (aka interventions) grows and dies even quicker. The FDA may approve tens of drugs a year that have been under study for a decade, and there is no equivalent for cybersecurity products.

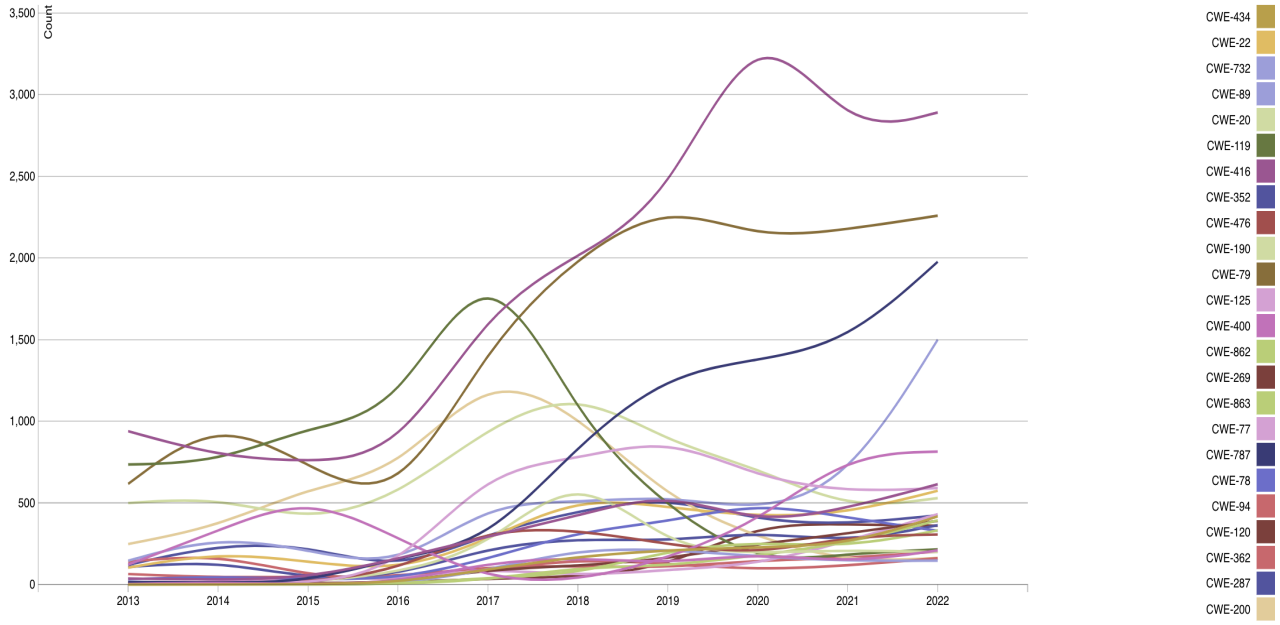


Figure 6.1: NIST CVE database of types of attack growth by year.[5]

The above shows a massive growth in 'unknown' types of attacks as the leading cause of CVEs starting in 2018. Each other family below is a known type of vulnerability, speaking to the challenge of defense, and utility of the database in coordinating response and knowledge-sharing. This evidence supports ***H3*** as cause for adversary efficacy.

[5]"Known CVE Database Dashboard." NVD - NIST.

7 Case Studies

7.1 Good Compliance Examples

This section will support ***H1***, which describes that organizations are not to blame, the latency of framework updates are at fault.

7.1.1 Intel Breach

Intel, one of the world's largest microchip manufacturers, partnered with NIST for a case study in the efficacy of the risk-reduction outcomes of the framework compared to their internal 'maturity model' framework, and the overlap between the two enough to denote themselves as 'NIST compliant'.[1]

Intel is 27001 compliant, will continue to be, have been for many years.[2] There are many more frameworks by which Intel ensures it adheres to. For these reasons and more, peer review organizations like Gartner continue to rank them highly in their supply chain security.

Despite these controls in place, which many know Intel possesses the personnel and finances to ensure their teams are of top-notch capabilities, they suffered a significant breach in mid-2020.[3]

This breach is the worst-case scenario, resulting in over 20Gb of their proprietary data including: flash tooling for various chips, BIOS reference/ sample/ initialization code, bootloader development, silicon source code, internal debugging and development tools, product roadmaps, binaries for SpaceX cameras, schematics of unreleased chips, processor simulators, and more.

This breach occurred due to a misconfiguration, where an attacker found this server on the open internet, tried default passwords on the server, and accessed all the files. Although there are controls

[1] "Uses and Benefits of the Framework." NIST, 16 Mar. 2023.
[2] "Intel Sourcing and Manufacturing Security Practices Overview." Intel.
[3] Goodin, Dan. "More than 20GB of Intel Source Code and Proprietary Data Dumped Online." Ars Technica.

in place to monitor the build, operation, and ongoing health of infrastructure, there is no compliance guide for why an organization *shouldn't* put sensitive files on the edge of their environment. The organization properly followed the framework guidance, procured the right types of setups, yet were woefully and blindly unprepared for a simple attack.

NIST's implementation tiers		Intel's maturity level–oriented tiers	
Tier 1 (partial)	**Tier 2 (risk informed)**	**Tier 1 (partial)**	**Tier 2 (risk informed)**
Risk-management process		**People**	
– Cybersecurity risk practices are informal – Cybersecurity priorities aren't informed by the organization's risk objectives	– Cybersecurity risk practices are approved – Cybersecurity priorities are informed by the organization's risk objectives	– Lack of cybersecurity training – Lack of awareness of security risks	– Employees have security training – Employees have awareness of risks and security resources
Integrated risk management		**Process**	
– Limited risk awareness at organization level – Practices are informal – Irregular implementation of security risk management	– Awareness of security risk at the organization level but not organizationwide – Risk-informed, management-approved processes are defined and implemented	– Informal risk management process – Lack of prioritization of threats into business decisions	– Cyberactivities are risk informed – Management processes are risk informed – Cyberrisk information is shared – Staff has adequate resources to perform cybersecurity duties
External participation		**Technology**	
– Lack of processes to coordinate and collaborate with other entities	– Firm knows its role but has no formal processes to coordinate and collaborate with other entities	– Lack of tools – Poor tool management – Inadequate tool deployment – Technology lags behind current threats	– Appropriate tools are deployed – Tools are maintained – Tools cover risk areas – Technology keeps pace with threats
		Ecosystem	
		– Lack of understanding of its role – No collaboration with external actors	– Firm understands its role – Firm collaborates with external actors on an ad hoc basis

Figure 7.1: Intel's maturity model matrix.[4]

7.1.2 Equifax Breach

Equifax is one of the largest credit reporting agencies in the world. Credit reporting exists as a mechanism to mitigate financial risk in small and business loans to unvetted people. It is a crucial aspect of acquiring homes, cars, and other resources that most people can't pay for upfront.

In order to verify identity, there is a long list of sensitive information contained in a reporting agency database, including: social security number, all previous addresses, income history, tax information, and more. This information could be used for identity theft, fraud, stalking/ harassment, and much more if given to the wrong parties.

Equifax prided itself with the right systems in place to be stewards of data. They were ISO27001 compliant years before the breach[5], and with that much time behind a certification, a reasonable assertion that they possessed a well-functioning team and organization.

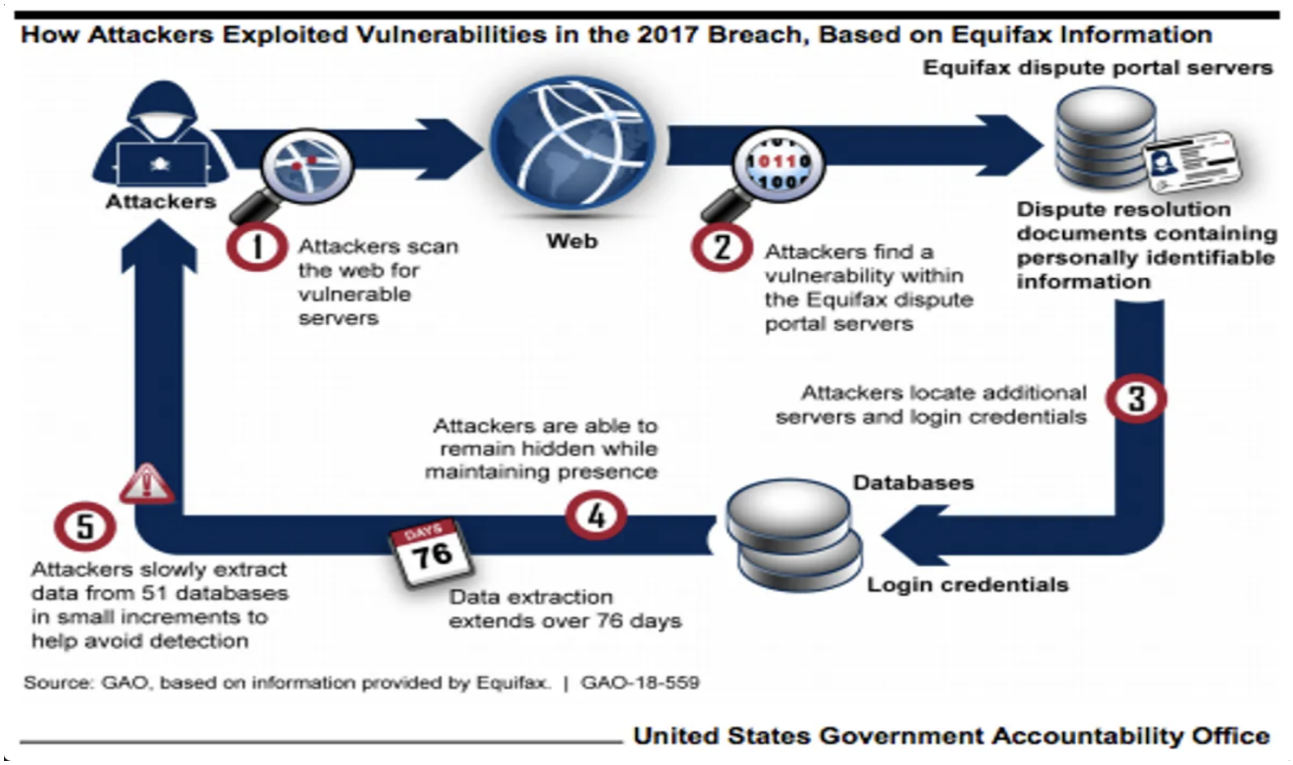


Figure 7.2: Equifax's breach analysis.[6]

[4]"A. Dedeke, "Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles," in IEEE Security & Privacy, vol. 15, no. 5, p52.

[5]"Equifax Held ISO 27001 Certification at Time of Massive System Hack." Oxebridge Quality Resources International, 22 Sept. 2018.

Regrettably, Equifax experienced a significant cyber breach in 2017[7], exposing the personal data of nearly 150 million Americans. The US Department of Justice (DoJ) in 2020 announced attribution to China PLA once again[8], and the Federal Trade Commission (FTC) is involved in paying out hundreds of millions in settlement dollars to affected persons.[9]

This breach occurred due to a failure to patch. CISA notified companies of a high-severity Apache struts vulnerability in early February. Equifax planned to patch this, and were negligent in doing so. Attackers discovered this external vulnerable server in March, gained access, and used their foothold to find more data-rich servers. Over the next 5 months, the adversaries successfully moved to the most sensitive data, and copied it to their machines over time to avoid detection.

There are compliance framework pieces that address monitoring tools, and personnel for them. Unfortunately, a compliance framework does not teach how to build an error-free process for validation. The frameworks contain no information on building a resilient, fault-tolerant architecture of product and personnel. Lastly, there are no lasting punishments for failure of due diligence, only financial impact from brand damage and settling in court.

7.2 Bad Compliance Examples

This section will support ***H2***, which describes that organizations are to blame, the latency of framework updates are not at fault.

7.2.1 Colonial Pipeline Ransomware Incident

The colonial pipeline is a South-East US gas pipeline stretching across many states from Florida up to Maryland. In the event of an outage, this single pipeline accounts for almost 10% of gas in the region across the 8 states it supplies.

Although Colonial Pipeline is part of the oil and gas industry, at the time of the attack there were no specific requirements for cybersecurity frameworks. This attack ultimately became a national security threat, leaving many Americans stranded and panicking for gas.

---

[6]"August 2018 Data Protection - Elizabeth Warren." Government Accountability Office (GAO), Aug. 2018.
[7]Ng, Alfred. "How the Equifax Hack Happened, and What Still Needs to Be Done." CNET, 7 Sept. 2018.
[8]"Chinese Hackers Charged in Equifax Breach." FBI, 10 Feb. 2020.
[9]Newman, John, and Amy Ritchie. "Equifax Data Breach Settlement." Federal Trade Commission, 20 Dec. 2022.

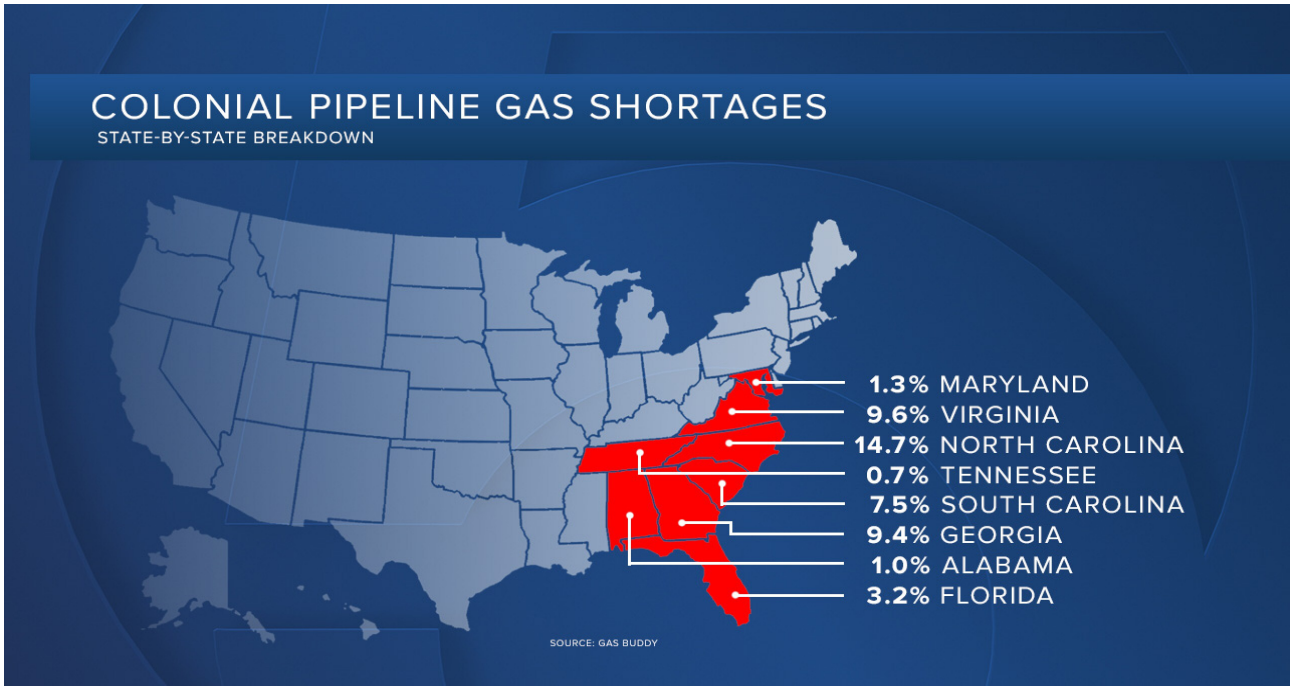


Figure 7.3: A map of Colonial Pipeline's supply route.[10]

Since 2019, the company exhibited bad compliance hygiene, not documenting network testing and alarm requirements. Since as early as 2017, employees were not entering data into the system due to its faulty displays and application crashes.[11]

The breach originally began with a remote employee's credentials of a re-used password. The employee used a password associated with the same username of a different breach, and the attackers got lucky with a dictionary attack on a virtual private network (VPN) server that did not log all attempts, nor were there multi-factor (MFA) prompts upon successful entry.[12] The IT organization were unaware the VPN was exposed in this way, no plans to patch or change its exposure, nor were there any initiatives to do so externally.

Colonial Pipeline was extorted 75 bitcoin (BTC), about $4.4M at that time. They opted to pay the

[10]CATHY BUSSEWITZ, BEN FINLEY and TOM FOREMAN. "Colonial Pipeline Restarts Operations Days after Major Hack." WPTV News Channel 5 West Palm, 12 May 2021.

[11]Nair, Prajeet, and Ron Ross. "Colonial Pipeline May Have to Pay Fine of Nearly $1 Million." Bank Information Security, 10 May 2022.

[12]Kerner, Sean Michael. "Colonial Pipeline Hack Explained: Everything You Need to Know." WhatIs.Com, 26 Apr. 2022.

ransom, against the official stance of US policy, to return to function as soon as possible.[13] Although the DoJ recovered most of this money, the attackers sure won on the day getting away with a few million dollars without attribution.

This failure stands out in many ways. It is a critical service to the citizenry, it covers a large terrain, and there aren't nationwide disaster recovery plans between private sector entities. There were no outside pressures for cybersecurity compliance, no internal cybersecurity champions, and still no lasting negatives to those responsible for this breach.

7.2.2 OPM Database Breach

The Office of Personnel Management (OPM) is the office tasked with maintaining records of the top secret/sensitive compartmented information (TS-SCI) certifications within the US. In order to gain a clearance, a prospect fills out a SF-86 form, which contains hundreds of pages of sensitive information including: all contacts, foreign friends, previous addresses, social security information, fingerprints, and more.

This breach resulted in the inadvertent disclosure of 22 million government personnel records, with nearly 400,000 TS-SCI persons identified in the breach.[14]

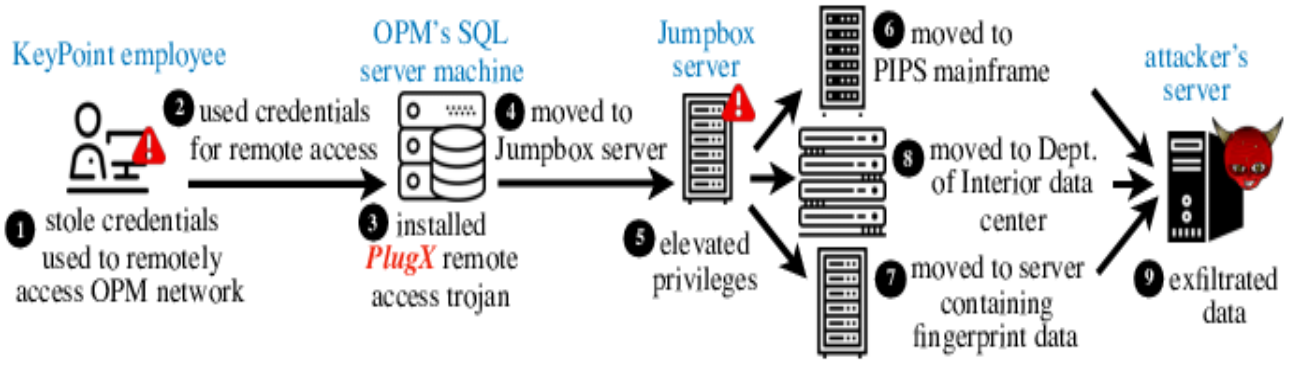


Figure 7.4: Anatomy of OPM breach stages.[15]

[13] Kelly, Stephanie, and Jessica Resnick-Ault. "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators." Reuters, 9 June 2021.

[14] Levine, Mike. "22 Million Affected by OPM Hack, Officials Say - University of Central ..." ABC News, 5 July 2015.

[15] Saleem, Hamza. "United States Office of Personnel Management (OPM) Data Breach, 2014 ..." ResearchGate.Net, Oct. 2020.

The OPM suffered minor breaches twice before[16] the large one. Since 2009, and every few years following, the inspector general of OPM included inadequate security practices in their assessments.[17] There were no punishments for this, nor were there any proposed fixes from congressional oversight bodies. Because of this negligence, there is ongoing civil liability class action suits unfolding.[18]

This breach used stolen credentials from a contractor to gain remote access to a single server, which then was used as the jump point to launch more sophisticated attacks across the infrastructure, and then exfiltrate the data out of the network.

These contractors were in use due to decreased budgets, the OPM teams needed to outsource part of their vetting processes. These contractors did not practice proper cybersecurity hygiene, built their infrastructure on a very minimal budget, and no oversight or investigation into their capabilities prior to entering business proved to be a huge blind spot. Ultimately, they were the weakest point.

To date, there are no compliance mandates that require frequent pentesting, that allow for purchasers of a product to see the results of pentest before entering into business with a contractor, and others. There's a blind spot to operational controls which are intentionally obscured by businesses to the outside world. While this remains true, there will be more blind spots exposed by attackers in the OPM breach way.

7.3 Compliance-Irrelevant Examples

This section will support ***H3***, which describes that neither organizations nor policymakers are to blame, cybercriminals are just that talented.

7.3.1 Kaseya Ransomware Incident

Kaseya is an IT vendor that provides solutions to monitor, manage, and protect digital infrastructure at scale, not unlike SolarWinds. However, unlike SolarWinds, Kaseya VSA software is targeted toward endpoint management to ensure laptops/computers/mobile devices are patched, and provide views into each network for which devices exist where.

---

[16] Sean Gallagher - Jun 16, 2015 7:22 pm UTC. "Encryption 'Would Not Have Helped' at OPM, Says DHS Official." Ars Technica, 16 June 2015.

[17] Lee, Timothy B. "The Devastating Hack of the Federal Office of Personnel Management, Explained."

[18] "Cybersecurity Resource Center: OPM Breach." U.S. Office of Personnel Management.

Kaseya are well along their compliance posture, with data residency in the EU, are mandated to be GDPR compliant as well as are ISO27001 compliant, and complete SOC2 type 2 audits regularly.[19] Many of Kaseya's largest customers are managed security service providers (MSSPs) which provide outsourced security and infrastructure management to small/medium-sized businesses all over the world.

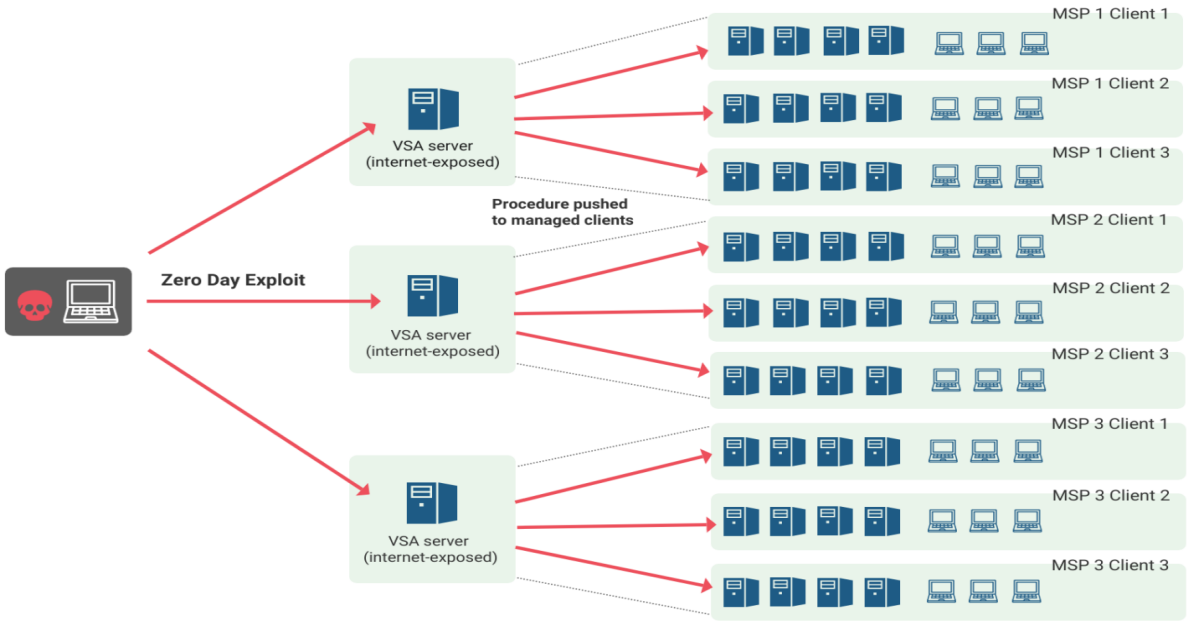


Figure 7.5: Kaseya MSSP malware deployment example.[20]

In July of 2021, Kaseya products were targeted by nation-state adversaries as an entry point to many networks. Although fewer than 60 customers of Kaseya were breached, this resulted in nearly 1,500 'downstream' businesses of the MSSPs, as the attackers leveraged the Kaseya management tool as a deployment mechanism of malware.[21]

A compliant company, with customers that are of varying degrees compliant, were unable to prevent a 0-day that ultimately spread far across the globe. It's particularly challenging to identify previously known-good behavior as malicious, especially if they are a part of your monitoring tools.

[19] "Earning Your Trust." Kaseya, 8 May 2023.
[20] Wadhwani, Sumeet. "Is Revil's Latest Exploit against Kaseya One of the Biggest Ransomware Attacks Ever?" Spiceworks, 23 July 2021.
[21] "Incident Overview & Technical Details – Kaseya." Kaseya Helpdesk.

8 Summary

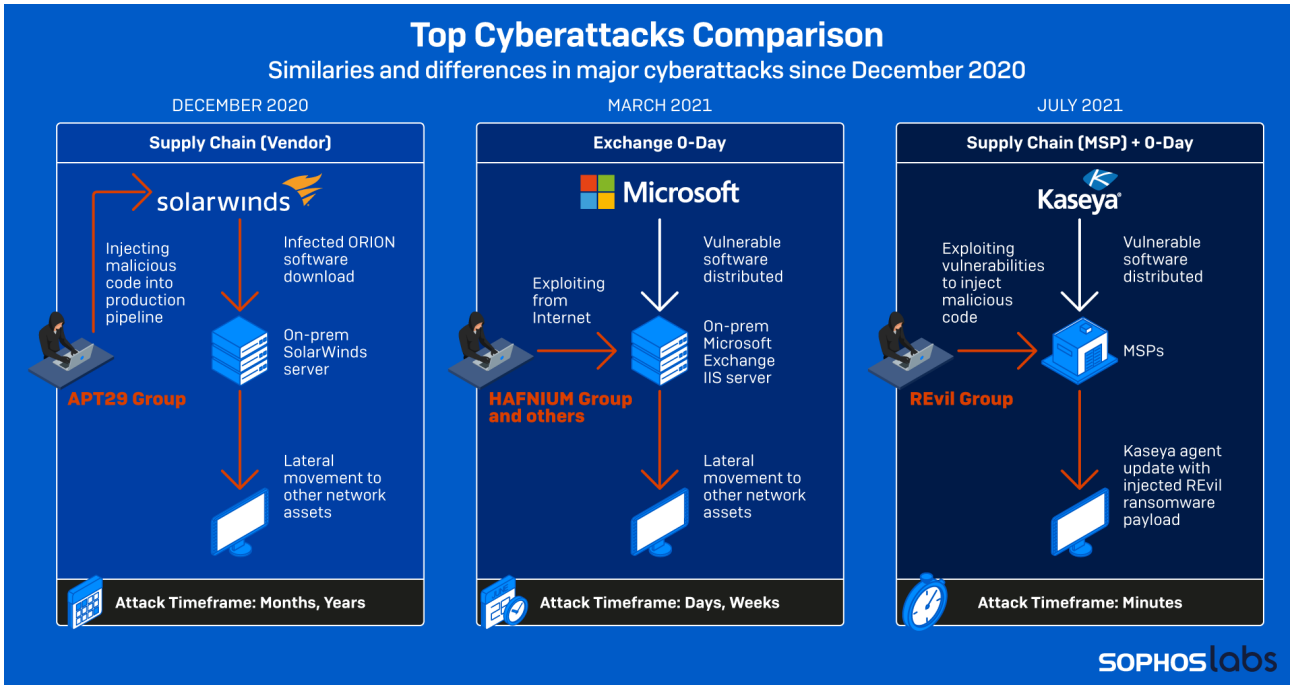


Figure 8.1: Large breaches comparison.[1]

There are compelling arguments on each side of this argument. If a cybersecurity framework is effective, why are compliant companies getting breached? However, there are companies of varying stages of compliance getting breached, does that mean the organizations are to blame? Or is it easier to point to the constant ingenuity of attackers?

In the previous sections, we've explored the growing challenges of expanding attacker capabilities. Case studies show various outcomes depending on cyber strategy, and the next section ties changes to frameworks to the breaches described above.

[1]Merry, Anthony. "Kaseya VSA Supply Chain Ransomware Attack." Sophos News, 8 Sept. 2021.

THIS PAGE LEFT INTENTIONALLY BLANK

Part IV

Findings

9 Updates Compared to CVEs

Based off the dates of publishing, there's significant overlap of published revisions to frameworks. The first update of ISO27001 contains most of the first update to SOC2. The first update of SOC2 contains most of the first update to NIST. The most recent version of ISO27001 contains all of the updates to SOC2 and most of NIST.

Therefore the analysis will be ISO27001 update 1, gap analysis of SOC2 update 1, gap analysis of NIST update 1, ISO27001 update 2, and then NIST gap analysis as inclusive of the other framework revisions. However, the NIST update 2 is unpublished at this time.

As a reminder, ISO27001 is a non-technical guide, and most organizations use ISO27002 as the guide for achieving ISO27001 compliance. Where possible, CVEs will be attributed to *technical controls*, likely coming from ISO27002. Denotions of change sources will be made below.

9.1 CVE Analysis

We will create a linear regression to anticipate how many of CVEs from 2005 were used in breaches up until 2021 using the exploited CVE database as the seed data.

9.1.1 Regression

JSON output of all CVEs, scores, and data by year is maintained by NIST NVD. Flattening the JSON and outputting to CSV code is in the Appendix. The data available for the known exploit database are below.

[2] As of 31 July 2023

Year	Total CVEs	Known Exploited CVEs
2023	16,401[1]	49
2022	23,897	115
2021	21,846	187
2020	20,254	130
2019	16,911	106

Table 9.1: Known exploit compared to total exploit counts
[2]

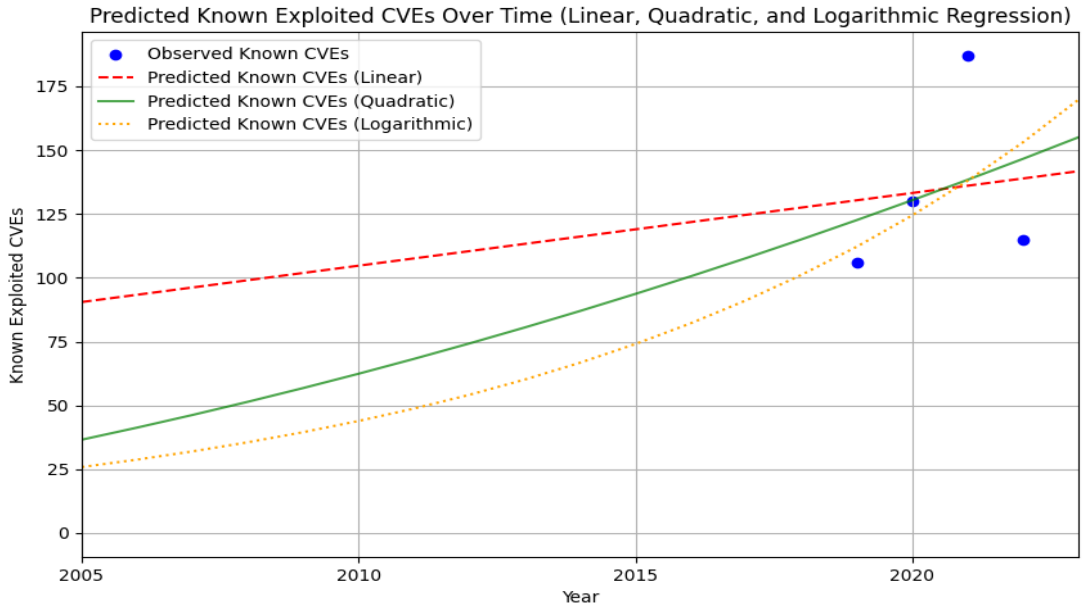


Figure 9.1: Plot of all regressions.

The linear regressions below assume known CVEs to be 0 in 1973, the credit of creation of the first personal computer and also omits 2023 as the incomplete year artificially lowers the slope. The data we have entries for, manually accounted for, will be in normal black text and all other additions from math will be highlighted.

[2]"NIST CVD." NVD.
[3]2023 data as of 31 July 2023, subject to change.

Year	Total CVEs	Linear Regression	Quadratic	Logarithmic	Average
2023	16,401	49	49	49	49
2022	23,897	115	115	115	115
2021	21.846	187	187	187	187
2020	20,254	130	130	130	130
2019	16,911	106	106	106	106
2018	16,970	115	115	101	**110**
2017	16,891	112	108	91	**104**
2016	10,542	109	101	82	**92**
2015	8,722	106	94	74	**91**
2014	8,974	103	87	67	**86**
2013	6,705	100	81	60	**80**
2012	5,855	96	74	54	**75**
2011	4,835	93	68	49	**70**
2010	5,201	90	62	44	**65**
2009	5,030	87	57	40	**61**
2008	7,175	84	51	36	**57**
2007	6,580	81	46	32	**53**
2006	7,143	78	41	29	**49**
2005	4,766	75	37	26	**46**

Table 9.2: Regression estimates (highlighted) of known exploited CVEs per year.
[3]

9.1.2 Heatmap

Further analysis and research will be required. An algorithm to crawl through all CVEs and the hundreds of datapoints they share to be predictive on previous and future likely attack vectors. To date, building a heatmap for the purpose of this study is out of scope but would allow for trending analysis on which characteristics of CVEs make them likely to be used in large attacks.

Essentially, scientists who predict the most likely variant of the flu each year is the intended outcome of this algorithm, based off the metrics we collect about current CVEs. Or perhaps identifying which datapoints are still required to make predictive analysis possible.

9.2 Gap Analysis

9.2.1 ISO Update 1

Window start date: **15 OCT 2005**, window end date: **31 OCT 2013**.

Changes Let's start with the technical control changes to 27002, and what that meant for policy changes.

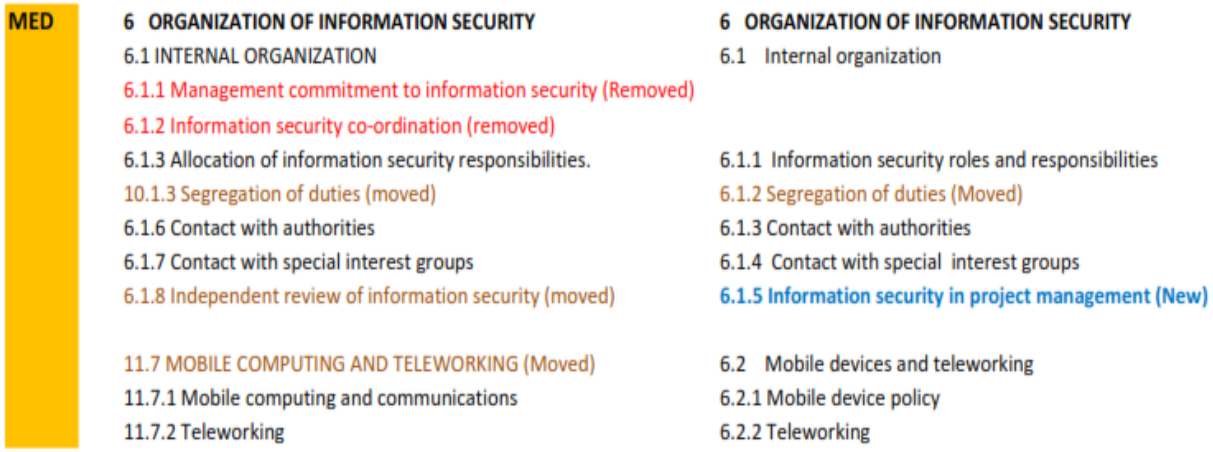


Figure 9.2: Technical control changes between 2013 and 2005 versions of ISO27002.
[4]

ISO removed references to management and board inclusion within protection strategy. Ultimately, they saw governance needs to be contained within the team responsible for implementing it, and the removal of co-ordination went into the policy side. You are also able to see where information security in project management came in, which imbues security by design during the development process. There were many additional subpoints within controls introduced.

A specific control example is against malware, page 40-42 in both versions of 2005 and 2013. The latter version added many different items, including "isolating environments where catastrophic impacts may result."

[4]Lineman, David. "ISO 27002:2013 Change Summary Heatmap." Information Shield.

Interestingly, ISO is also now aware of unpatchable/fixable devices in production, adding in: ”define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.”

Assessment ISO is aware of significant adverse consequences of technology in production environments and the need to change them. There are many attacks at this time that were high profile against governments. The Shadow Network attacking Indian, Australian, and US Government entities proved there were significant infrastructure and operational changes required. Specifically, StuxNet and other case studies prove that the specific recommendation changes are a best-effort attempt for risk mitigation augmentation in light of cyber threat evolution.

That is to say, attacks against flat networks that were successful changed the scope of recommendations in compliance to prove access authentication and flat networks were no longer in place.

9.2.2 SOC2 Update 1

Window start date: **15 APR 2010**, window end date: **1 DEC 2017**.

Changes A larger facelift compared to peer framework revision 1’s, AICPA changed from ’Trust Service Principles’ to ’Trust Service Criteria’ which includes alignment to the COSO standards, and provides further emphasis on risk mitigation for cybersecurity across 4 broad categories:[5]

1. logical and physical access controls
2. system operations
3. change management
4. risk mitigations

As a reminder, SOC2 is completed by CPA’s, and are non-technical in nature, below is an example report and findings:

[5]Nyman, Mike. “New SOC 2 Report Framework Addresses Emerging Risks.” CLA Connect, 2018.

Criteria Number	Criteria Details	Controls Specified by ACME Corp.	Test Results	Management Response
1.1	Entity demonstrates a commitment to ethical values.	–	Exception noted.	Management have a process in place to review ethical alignment.
1.2	Management establishes, with board oversight, structures, appropriate authorities and responsibilities, and rules for responsibilities in the pursuit of objectives.	–	Exception noted.	ACME are building a board oversight committee.
1.3	The entity demonstrates a commitment to attract, new hires and retain competent individuals in onboarding alignment with objectives.	ACME put a talent acquisition team in place to attract and retain new members.	For 1 in 45 hires, the retention program was ineffective.	ACME will perform more frequent reviews of policy acknowledgements for new hires in the future.
5.3	The entity deplovs control activities through policies that establish what is expected and in procedures that put policies into action.	The policy establishes roles and responsibilities and rules for achieving goals, all new hires are to read it.	2 of 45 new hires were provided this much after hire date.	Management are reviewing information distribution tools.

Table 9.3: Example SOC2 Type II Report.

Assessment SOC2 put specific controls in place, CC6,7,8, and 9 for the above 4 bullet points. Addressing physical access auditing to buildings, system operation in real-time, how changing operational requirements and behaviors are documented, and what is being done in the meantime to address

outstanding risk.[6]

For example, CC6.6 reads *Every Production host is protected by a firewall with a deny-bydefault rule. Deny by default rule set is a default on the Entity's cloud provider*. This is behavior that emulates Kindervaag's Zero Trust Framework, starting prior to this update. It is then concluded specific threats shown to exfiltrate data are correlated to these revisions. However, a CPA conducting this assessment might not understand how applications are identified on a firewall, how these technologies are able to be fuzzed, and other technical implementation details (decryption). An entity may pass without actually completing technical validation, with blind spots and caveats in rulebases.

Attacks utilizing misconfigured devices, unpatched devices, devices missing protective software do correlate strongly to many of the changes described in SOC2 Type II report updates, aligned to the SolarWinds case study.

9.2.3 NIST Update 1

Window start date: **12 APR 2014**, window end date: **16 APR 2018**.

Changes NIST focused their efforts to improve strategy in 4 key areas[7]:

1. authentication and identity
2. self-assessing cyber risk
3. managing supply chain cybersecurity
4. vulnerability disclosure

Specficailly, NIST added the concept of and better accounts for emerging vulnerability information (i.e., Coordinated Vulnerability Disclosure). A new subcategory related to the vulnerability disclosure lifecycle was added to Analysis under the Respond function because organizations need to incorporate vulnerability data and identify emerging risks and use cyber threat information from internal and external sources to gain and facilitate a better and more robust understanding of the likelihood and impact of cybersecurity events.[8]

---

[6] "2017 Trust Services Criteria (with Revised Points of Focus – 2022)." AICPA.

[7] "NIST Releases Version 1.1 of Its Popular Cybersecurity Framework." NIST, 16 Apr. 2018.

[8] Albrycht, Elizabeth. "11 Jan Summary of Pending NIST Cybersecurity Framework (CSF) Changes in Version 1.1 Draft 2." Criterion Systems, 11 Jan. 2018.

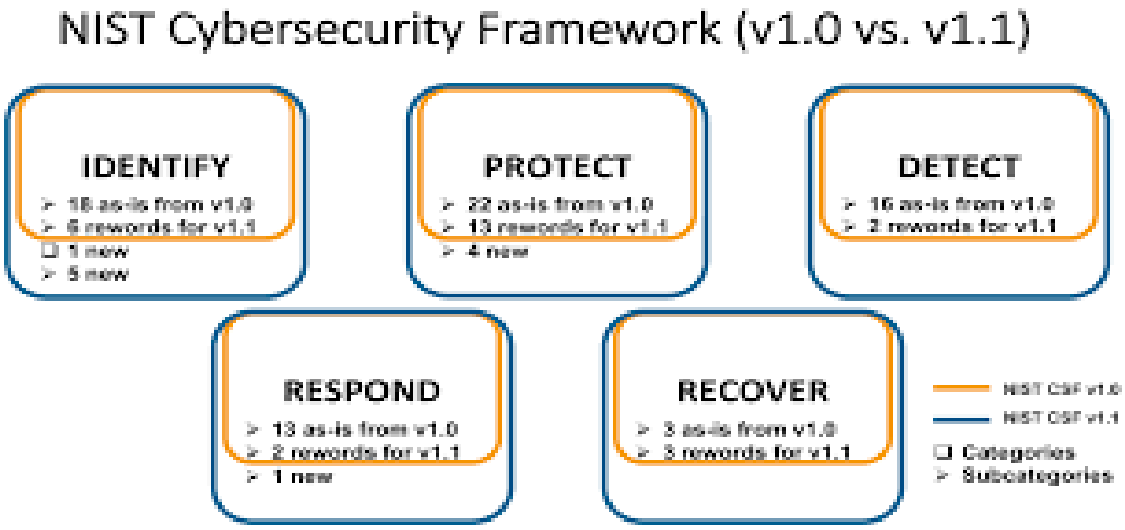


Figure 9.3: Categories and subcategory changes of NIST CSF 1.1 revision.
[9]

NIST also added a new Cyber Supply Chain category under the Identify function and added 5 new subcategories. The primary objective of cyber supply chain risk management (SCRM) is identify, assess, and mitigate cyber-related products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within supply chain. Enhanced Section 3.3 guidance for applying the CSF for SCRM including management of cybersecurity within supply chains and for acquisition decisions, as well as updated entity diagram and taxonomy. Incorporates supply chain considerations into the "External Participation" property of Implementation Tiers.[10]

Assessment This is a year of big change to the perspectives of cybersecurity risk. CISA needing to assist in triage of breaches of Target, Home Depot, the DNC, while also watching WannaCry, the Ukrainian power grid, and Georgia all fall victim to various ransomware groups. The two biggest changes were in direct response to a lack of awareness of many teams. Coordinating vulnerability management into everyday decision making, as well as incorporating service provider/vendor risk into purchasing decisions (necessitating compliance adhesion).

[9]Boeckmann, Chad. "Changes between NIST CSF 1.0 to NIST CSF 1.1 - Trustmapp: Cybersecurity Performance Management." TrustMAPP, 13 June 2018.

[10]Albrycht, Elizabeth. "11 Jan Summary of Pending NIST Cybersecurity Framework (CSF) Changes in Version 1.1 Draft 2." Criterion Systems, 11 Jan. 2018.

These findings are consistent with the OPM breach case study, in that adoption of risk mitigation for purchasing and use discourse is lacking in the industry at scale.

9.2.4 ISO27001 Update 2

Window start date: **31 OCT 2013**, window end date: **25 OCT 2022**.

Changes The scope of ISO/IEC 27001:2022 changelog[11] includes:

- 11 new controls
- 57 controls merged
- 23 controls renamed
- 3 controls removed

This tracks with the general understanding that revisions to 27001 are mostly in definitions, to reduce complexity in the planning, process execution, and monitoring standards criteria.

Figure 9.4: Controls introduced into ISO27001:2022.
[12]

[11] Lubbert, Adam. "ISO 27001:2013 vs ISO 27001:2022: CSA."
[12] Kosutic, Dejan. "What Are the 11 New Security Controls in ISO 27001:2022?" 27001Academy, 20 Jan. 2023.

Assessment The control changes address specific threats introduced by novel attack vectors through the last 9 years. Specifically addressing lacking coordination among defenders through threat intelligence, and data loss prevention tools inline coupled to web filtering given the prevalence of SaaS during COVID. Not unlike NIST, improvements to secure coding and requirements for it specifically call attention to supply-chain security, and mitigating risk to all customers.

Lessons learned from Kaseya, SolarWinds, Microsoft, and more align to the second hypothesis that controls update well but organizations are slow to take them up.

9.2.5 NIST Update 2

Window start date: **16 APR 2018**, window end date: **– AUG 2023**.

Changes There are a few major changes and minor proposed changes to the successful framework. NIST will add a new category, govern, to facilitate better recommendations and adhesion between IT practitioners and oversight personnel.

Figure 9.5: NIST CST 2.0 proposed pillars.
[13]

NIST CSF 2.0 updates aim to:

[13] Kimmerle, Kris. "Quick Analysis of NIST CSF 2.0." LinkedIn, 8 May 2023.

- Cybersecurity outcomes applicable to all organizations, removing language specific to critical infrastructure across the Core;
- The prevention of cybersecurity incidents through outcomes focused in Govern, Identify, and Protect Functions and the detection and response of incidents through the Detect, Respond, and Recover Functions;
- Cybersecurity governance through a new Govern Function covering organizational context, risk management strategy, policies and procedures, and roles and responsibilities;
- Cybersecurity supply chain risk management outcomes;
- Continuous improvement through a new Improvement Category in the Identify Function;
- Leveraging the combination of people, process, and technology to secure assets across all Categories in the Protect Function;
- Resilience of technology infrastructure through a new Protect Function Category; and
- Cybersecurity incident response management, including the importance of incident forensics, through new Categories in the Respond and Recover Functions.

Assessment There are specific additions proposed like ID.IM-01: Continuous evaluation, including through reviews, audits, and assessments (including self-assessments), is applied to identify opportunities for improvement across all framework functions. Governance includes changes like: GV.RR-01: Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement. There are minor changes from requirements like ”inventory is catalogued” to ”inventory lists are maintained” which implies we are moving away from checklists and towards operational outcomes.[14]

The specific proposals are to mitigate the challenge proposed in research questions, which organizations use to be compliant without operationalizing lessons. This puts stakeholders in place for repeated exposure, accountability from executives, and others. Lessons learned from breaches with Marriott, Facebook, Capital One, and even some of the case studies (Kaseya, most notably).

[14]“Discussion Draft of the NIST Cybersecurity Framework 2.0 Core.” NIST.

9.3 Summary

The frameworks all established correlational relationships with known exploited CVEs, successful hacks, and theoretical research documenting changes in efforts to overcome the challenges evolution presented. The case studies largely supported this statement.

The research is inconclusive on the causal relationships between CVEs and compliance frameworks, further study on the revision motivations required to properly establish this tie. It is shown that revisions are covering new CVE techniques and outcomes, however, this correlation is less well supported due to lack of data.

Further research required to establish predictive analysis on relation of CVE characteristics to successful breaches and eventual framework changes. Another beneficial research direction may be to analyze MITRE ATT&CK framework for timelines of added techniques, correlated to new CVEs, which then would be more philosophical/behavioral analysis of outcomes opposed to technical controls.

Framework	CVEs During	New Controls	New Technical	Technical From CVEs
ISO 2005	-	114	63	-
ISO 2013	46,585	-	-	-
ISO 2022	127,815	11	7	4
NIST 1.0	-	108	52	-
NIST 1.1	45,129	10	-	-
NIST 2.0	99,878	38	10	3
SOC2 2010	-	64	14	-
SOC2 2017	50,834	4	2	1
SOC2 2022	92,872	4	-	-

Table 9.4: Control counts by introduction version.

10 Hypothesis Alignment

As a reminder, the original research question is *"To what extent does the latency of updates to cybersecurity compliance frameworks impact efficacy of organizational cyber risk mitigation?"*

This question's hypothetical answer is "Yes there is a latency-induced effect, and here's why:"

H1 The frameworks are useful, but aren't current enough. The policymakers are to blame.

H2 The frameworks are useful, regardless of latency. The organizations are to blame.

H3 The frameworks aren't useful, regardless of latency. The attackers are to blame.

10.1 Case Study Analysis

Few companies fall within the scope of "compliance" across any of the frameworks. Many find themselves on a long and incomplete journey, and only the largest are able to dedicate proper resources to achieving and maintaining these. Intel and Equifax case studies documented critical failings in the recommendations of compliance frameworks due to their inability to think broadly about operations opposed to checking boxes. The certifying bodies are to blame, or rather, used to be. They've since updated, but, at the times of the breaches, can be partially to blame.

Most companies fall into a scope of bad compliance. Most businesses that are unable or unwilling to retain skilled staff dedicated to compliance, especially given the technical acumen required to demonstrate compliance is already in high demand maintaining expiring infrastructure in contrast to growing digital operation need. Colonial Pipeline and OPM case studies documented the lived experience of most companies, their inability to complete compliance frameworks as they exist today, regardless of the contents of the frameworks.

The last hypothesis places blame on the attackers, who will continue to ”always find a way.” This will always be true, and represent the edge case of breaches. Most breaches are from reused passwords without MFA in place, and unpatched/unmonitored web servers with flat networks behind them. Essentially, we are making it too easy for them most times.

10.2 Other Source Analysis

The UK government publishes annual breach reports, which 2023 documents interesting trends. Their conclusions show smaller businesses and charities may be increasingly cash-poor and don't spend as much time with analytics and reporting of breaches. The study corroborates the majority of breaches occurring due to an unsophisticated adversary, motivated by money, and there being insufficient controls in place for passwords and access.[1]

This is not the only study to criticize smaller businesses and their incomplete response options and perspectives in contrast to an automated adversary. The review of MIT, MITRE, Mandiant, and most vendor sources do show skillful adversaries, but, the majority of organizations threat model isn't inclusive of this, and the threat model they should be concerned with ultimately is not being adequately responded to, either.

10.3 Summary

While each hypothesis possesses case studies, vendor/academic data, and other source analysis in support of it the numbers tell a different story. The data denotes most organizations worldwide are not currently delivering on any compliance objectives, nor have the resources to.

This firmly supports the answer that latency to framework updates does have correlational effects toward attacker/defender efficacy within their organizations, but wholly, these organizations are to be blamed for not undertaking their compliance requirements. ***H2***

The conclusion will describe takeaways, recommendations, and mitigations to ensure that victim-blaming can't be the only response to a wholly inadequate cybersecurity governance industry.

[1]Johns, Emma, and Maddy Ell. “Cyber Security Breaches Survey 2023.” GOV.UK, 19 Apr. 2023

THIS PAGE LEFT INTENTIONALLY BLANK

Part V

Conclusion

11 Known Limitations

The known CVE database is from 2021-onward, and any entries within it are dated in the sense that while there are 2019 CVEs there, in 2019 CVEs from 2017 might be most prominent. The data does not exist to properly correlate which attacks are of highest success, beyond knowing password reuse and lack of MFA is the fault of most attacks, second being CVEs on webservers.

The dataset of known breaches, and known attacks, is generally thought to be much smaller than what is actively occurring. There aren't legal ramifications in most places for not disclosing, nor lacking compliance in security posture.

The relationship between known CVEs and framework policy revisions is correlational, there are some direct ties between how a notorious attack and updates which are noted, but by and large it is difficult to establish causality.

Because of these factors, this study should not be taken to mean "the question is answered, apply it broadly to the entire industry." However, it can be stated plainly that compliance frameworks, to their credit, are aware of emerging threats and act accordingly.

Further study is required to establish the true causality chain of attack and prevention changes, and more data will be required to make more accurate predictions, as well as useful takeaways for the industry as a whole. To date, there is not enough leadership in government to compel private sector actors to contribute all their data, and until these barriers are removed and companies are required to do so, it is unlikely these outcomes will be changed.

12 Questions Unanswered

If every corporation becomes compliant, and breaches are still occurring with regularity, does that support H1 or H3 more? It will be difficult to research the answer because there are many company-specific and environment-specific reasons why compliance doesn't equate to security. However, it diminishes the value of compliance, most certainly.

If the above is answered by H1, what options are there beyond compliance to effectuate better cybersecurity? Ultimately this is an operations question. If compliance frameworks are designed to be preventative (as they are now), then they will continue to fall flat during a breach. There isn't a way around this until we change the goals of compliance away from decision-making centering around prevention to outcomes.

If the above is answered by H3, what options are there beyond compliance to disadvantage the attackers? The answers from here get more worrisome, as the simple answer may be to diminish the capabilities of a free and open internet. The best answer might be nationalization or coordination of all resources in a meaningful way, however, this is very unlikely.

If compliance frameworks are shown to not equate to secure operations, should companies become compliant? Yes, these are the best ways we are able to show diligence and planning for better outcomes, today. While they are not the best, they are what most are able to reach for. In the next section we will discuss what that means for organizations.

13 Recommendations

The data largely supports organizations are too slow at implementing compliance systems for it to be effective ***(H2)*** against an increasingly coordinated and automated adversary. There are effects of the latency of the frameworks themselves, but, these effects are small compared to the pressure organizations put themselves under becoming compliant in bad faith.

13.1 Practitioners

Most compliance checks do not properly ascertain the true risk posture of an organization. While it is easy to show a firewall possesses a default block rule at the bottom of the ruleset (explicit deny), CPAs aren't necessarily checking potentially thousands of rules, ports, and applications to logically separate the types of traffic allowed. Organizations may not be decrypting it for legal or technical reasons. There are many hairs to split in the compliance checks across the entire list.

The CISO for most organizations does not report directly to the CEO. Usually a CIO, and sometimes the CIO sits under the COO. Until there is actual accountability at the highest levels of the office, and above as mentioned the real risk assumed with the chosen deployment, attackers will succeed.

There is no punishment for failure, there is no legal imperative to comply. Until these change, companies are not incentivized to do anything but gamble and think "it won't be us."

As such, practitioners are encouraged to provide regular threat and risk assessments, based in data of surrounding sectors, peer companies, and writeups for threat analysis pertinent to change within their own organization especially if there is risk of falling to the same. They are further encouraged to uplevel their presentation and exposure to the highest offices, and seek continued counsel with the correct decision-makers where possible.

13.2 Defenders

Defenders specifically possess challenges practitioners might not. Defenders ultimately are responsible for prevention and detection of threats, and likely general infrastructure changes as well. It's worth communication with teams outside of IT the risks of the tools that are used, as well as positioning IT as the final say for all tools in use. Much like reducing attack surface by prevention of applications on your network, IT organizations are encouraged to not do business with teams that can't prove they are aware of compliance goals and are working to implement them in a good faith manner.

Secondly, practitioners are encouraged to not accept compliance in a bubble, but, ensure that regular pentesting and red team exercises are a part of the compliance checks, even where not required.

For most organizations that are too small to run security specific teams, attacking or defending, partnering with a good MSSP is the bare-minimum to ensuring there's telemetry and overwatch occurring in your environment. Compliance alone is not enough, operations need to improve, so outsource as a last resort. This will likely be the case for most organizations worldwide, so it is imperative for the correct incentives to be in place to make this transaction possible for organizations of any size, and continued in efficacy and growth in light of increasingly rare resources compared to business growth and expansion. Consolidating these skills to an effective place is imperative.

13.3 Observers

Consolidation seems to be the best way to get the most resources to the most people as possible. The attackers are following the same trends and seeing increased efficacy, so pressuring ISPs, government entities, and general bottlenecks of technical processing capability to act on behalf of organizations not possessing the same capabilities is important.

CISA and the DoD already do this for their own organizations with a detection tool called Einstein[1] and it's probably time we call for the same. In all areas of regional power, whether that is a parent-teacher organization, a youth sports league, a neighborhood collective... it is important we understand that our data will increasingly be used against us in a public and private way, and the companies holding it may not act in our best interest. So it's inherent to educate about risk, and prevent use where possible.

[1] `https://www.cisa.gov/einstein`

THIS PAGE LEFT INTENTIONALLY BLANK

Part VI

Appendix

A Acknowledgements

This paper was prepared and built in LaTeX, with numerous answers from Stack Overflow, and assistance from template libraries with open-source contributions from many.

B Code Snippets

JSON to CSV

```
import pandas as pd
import json
import os

def flatten_json(y):
    out = {}

    def flatten(x, name=''):
        if type(x) is dict:
            for a in x:
                flatten(x[a], name + a + '_')
        elif type(x) is list:
            i = 0
            for a in x:
                flatten(a, name + str(i) + '_')
                i += 1
        else:
            out[name[:-1]] = x

    flatten(y)
    return out

# Iterate over the years
for year in range(2005, 2022):
    # Define the file paths
    json_file_path = f'{year}.json'
```

```
    csv_file_path = f'{year}.csv'

    # Check if the JSON file exists
    if os.path.exists(json_file_path):
        # Load json data
        with open(json_file_path) as f:
            data = json.load(f)

        # Extract 'CVE_Items' list
        data_items = data['CVE_Items']

        # Flatten each item in the list and append to a new list
        flat_list = [flatten_json(item) for item in data_items]

        # Convert list of flat dictionaries to pandas DataFrame
        df = pd.DataFrame(flat_list)

        # Write DataFrame to csv
        df.to_csv(csv_file_path, index=False)
        print(f'Successfully converted {json_file_path} to {csv_file_path}')
    else:
        print(f'{json_file_path} not found')

```

Listing B.1: Python script to convert JSON to CSV

Linear Regression

```
import pandas as pd
import numpy as np
from sklearn.linear_model import LinearRegression
import matplotlib.pyplot as plt

# Data from the LaTeX table
data = {
    "Year": [1973, 2005, 2022, 2021, 2020, 2019],
    "Total_CVEs": [0, 4, 23897, 21846, 20254, 16911],
```

```
    "Known_Exploited_CVEs": [0, 4, 115, 187, 130, 106]
}

# Create a pandas DataFrame
df = pd.DataFrame(data)

# Linear regression
X = df['Year'].values.reshape(-1, 1)
y = df['Known_Exploited_CVEs'].values

# Create and fit the linear regression model
regression_model = LinearRegression()
regression_model.fit(X, y)

# Get the coefficients (intercept and slope)
intercept = regression_model.intercept_
slope = regression_model.coef_[0]

print("Linear Regression Equation:")
print(f"Known_Exploited_CVEs = {intercept:.2f} + {slope:.2f} * Year")

# Predicting known CVEs for each year from 1973 to 2023
years = np.arange(1973, 2024)  # Convert range object to NumPy array
years_array = years.reshape(-1, 1)

# Clip predictions to avoid negative values
predicted_known_cves = np.clip(regression_model.predict(years_array), 0, None)

# Output the results
print("\nPredicted Known Exploited CVEs for each year from 1973 to 2023:")
for year, predicted_cves in zip(years, predicted_known_cves):
    print(f"{year}: {round(predicted_cves)}")

# Create a plot to visualize the regression line and predicted known CVEs
plt.figure(figsize=(10, 6))
plt.scatter(df[df['Year'] > 2005]['Year'], df[df['Year'] > 2005]['
    Known_Exploited_CVEs'], color='blue', label='Observed Known CVEs')
```

```
plt.plot(years[years > 2005], predicted_known_cves[years > 2005], color='red',
    label='Predicted Known CVEs')
plt.xlabel('Year')
plt.ylabel('Known Exploited CVEs')
plt.title('Predicted Known Exploited CVEs Over Time')
plt.xlim(2005, 2023)  # Set x-axis limits to show only years from 2005 to 2023
plt.xticks(np.arange(2005, 2024, step=5))  # Set x-axis ticks as whole numbers
    from 2005 to 2023
plt.legend()
plt.grid(True)
plt.show()

```

Listing B.2: Python script for linear regression

Quadratic Regression

```
import pandas as pd
import numpy as np
from sklearn.linear_model import LinearRegression
from sklearn.preprocessing import PolynomialFeatures
import matplotlib.pyplot as plt

# Data from the LaTeX table
data = {
    "Year": [1973, 2022, 2021, 2020, 2019],
    "Total_CVEs": [0, 23897, 21846, 20254, 16911],
    "Known_Exploited_CVEs": [0, 115, 187, 130, 106]
}

# Create a pandas DataFrame
df = pd.DataFrame(data)

# Quadratic regression
X = df['Year'].values.reshape(-1, 1)
y = df['Known_Exploited_CVEs'].values

```

```
# Transform the features to quadratic features
poly = PolynomialFeatures(degree=2)
X_poly = poly.fit_transform(X)

# Create and fit the quadratic regression model
regression_model = LinearRegression()
regression_model.fit(X_poly, y)

# Get the coefficients (intercept and slopes)
intercept = regression_model.intercept_
slope_1 = regression_model.coef_[1]
slope_2 = regression_model.coef_[2]

print("Quadratic Regression Equation:")
print(f"Known_Exploited_CVEs = {intercept:.2f} + {slope_1:.2f} * Year + {slope_2
    :.2f} * Year^2")

# Predicting known CVEs for each year from 1973 to 2023
years = np.arange(1973, 2024)  # Extend the range for prediction
years_array = years.reshape(-1, 1)
years_poly = poly.transform(years_array)

# Clip predictions to avoid negative values
predicted_known_cves = np.clip(regression_model.predict(years_poly), 0, None)

# Output the results
print("\nPredicted Known Exploited CVEs for each year from 1973 to 2023:")
for year, predicted_cves in zip(years, predicted_known_cves):
    print(f"{year}: {round(predicted_cves)}")

# Create a plot to visualize the quadratic regression curve and predicted known
    CVEs
plt.figure(figsize=(10, 6))
plt.scatter(df['Year'], df['Known_Exploited_CVEs'], color='blue', label='
    Observed Known CVEs')
plt.plot(years[years >= 2005], predicted_known_cves[years >= 2005], color='red',
     label='Predicted Known CVEs (Quadratic)')
```

```
plt.xlabel('Year')
plt.ylabel('Known Exploited CVEs')
plt.title('Predicted Known Exploited CVEs Over Time (Quadratic Regression)')
plt.xlim(2005, 2023)  # Set x-axis limits to show only years from 2005 to 2023
plt.xticks(np.arange(2005, 2024, step=5))  # Set x-axis ticks as whole numbers from 2005 to 2023
plt.legend()
plt.grid(True)
plt.show()

```

Listing B.3: Python script for quadratic regression

Logarithmic Regression

```
import pandas as pd
import numpy as np
from sklearn.linear_model import LinearRegression
import matplotlib.pyplot as plt

# Data from the LaTeX table
data = {
    "Year": [1973, 2022, 2021, 2020, 2019],
    "Total_CVEs": [0, 23897, 21846, 20254, 16911],
    "Known_Exploited_CVEs": [0, 115, 187, 130, 106]
}

# Create a pandas DataFrame
df = pd.DataFrame(data)

# Logarithmic regression
X = df['Year'].values.reshape(-1, 1)
y = np.log1p(df['Known_Exploited_CVEs'].values)  # Apply logarithm to the target variable

# Create and fit the linear regression model
regression_model = LinearRegression()
```

```
regression_model.fit(X, y)

# Get the coefficients (intercept and slope)
intercept = regression_model.intercept_
slope = regression_model.coef_[0]

print("Logarithmic Regression Equation:")
print(f"Log(Known_Exploited_CVEs) = {intercept:.2f} + {slope:.2f} * Year")

# Predicting known CVEs for each year from 1973 to 2023
years = np.arange(1973, 2024)  # Extend the range for prediction
years_array = years.reshape(-1, 1)

# Logarithmic regression predictions
predicted_known_cves = np.expm1(regression_model.predict(years_array))  #
    Inverse of log transformation

# Output the results
print("\nPredicted Known Exploited CVEs for each year from 1973 to 2023:")
for year, predicted_cves in zip(years, predicted_known_cves):
    print(f"{year}: {round(predicted_cves)}")

# Create a plot to visualize the logarithmic regression curve and predicted
    known CVEs
plt.figure(figsize=(10, 6))
plt.scatter(df['Year'], df['Known_Exploited_CVEs'], color='blue', label='
    Observed Known CVEs')
plt.plot(years[years >= 2005], predicted_known_cves[years >= 2005], color='red',
     label='Predicted Known CVEs (Logarithmic)')
plt.xlabel('Year')
plt.ylabel('Known Exploited CVEs')
plt.title('Predicted Known Exploited CVEs Over Time (Logarithmic Regression)')
plt.xlim(2005, 2023)  # Set x-axis limits to show only years from 2005 to 2023
plt.xticks(np.arange(2005, 2024, step=5))  # Set x-axis ticks as whole numbers
    from 2005 to 2023
plt.legend()
plt.grid(True)
```

```
plt.show()

```

Listing B.4: Python script for log regression

LaTeX Keyword Extraction Script

```
import os
import re
from collections import Counter

# Step 1: Read the LaTeX file
script_directory = os.path.dirname(os.path.abspath(__file__))
file_path = os.path.join(script_directory, 'main.tex')

with open(file_path, 'r') as file:
    latex_content = file.read()

# Step 2: Extract text from LaTeX commands
command_pattern = r'\\[a-zA-Z]+\{([^}]*)\}'
extracted_text = re.findall(command_pattern, latex_content)

# Step 3: Remove LaTeX commands and special characters
cleaned_text = ' '.join(extracted_text)
cleaned_text = re.sub(r'\\[^a-zA-Z{}]+', '', cleaned_text)

# Step 4: Tokenize the text
tokens = re.findall(r'\b\w+\b', cleaned_text.lower())

# Step 5: Filter keywords (stop words)
stop_words = set([
    'the', 'and', 'is', 'of', 'in', 'a', 'an', 'for', 'to', 'on', 'with',
    'url', 'https', 'www', 'com', 'table', 'figure', 'fig', 'gov', '27002', '
    27001'
])  # Add more if needed

# Add numbers 1 to 10 and years 2005 to 2023 to stop words
```

```
stop_words.update(set(str(i) for i in range(1, 11)))
stop_words.update(set(str(year) for year in range(2005, 2024)))

filtered_tokens = [token for token in tokens if token not in stop_words]

# Step 6: Count keyword frequency
keyword_frequency = Counter(filtered_tokens)

# Step 7: Select top keywords (adjust the number as needed)
top_keywords = keyword_frequency.most_common(20)

# Step 8: Print keywords in terminal
print("Top keywords:")
for keyword, frequency in top_keywords:
    print(f"{keyword}: {frequency}")


```

Listing B.5: Python script for keyword identification

C References

C.1 Print

- A. Dedeke, "Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles," in IEEE Security & Privacy, vol. 15, no. 5, pp. 47-54, 2017, doi: 10.1109/MSP.2017.3681063.
- Bloomfield, Lincoln P., and Allen Moulton. Managing International Conflict: From Theory to Policy: A Teaching Tool Using CASCON. New York: St. Martin's, 1997. Print.
- Carr, Jeffrey. Inside Cyber Warfare. 2012. Print.
- Chapple, Mike, and David Seidl. Cyber Warfare: Information Operations in a Connected World. Burlington, MA: Jones and Bartlett Learning, 2015. Print.
- Cyber Security Review. 26 Mar. 2017.
- Modesti, Cristiana. "Incentivizing Cybersecurity Compliance in the New Digital Age: Prevalence of Security Breaches Should Prompt Action by Congress and the Supreme Court." Cardozo Arts & Ent. LJ 36 (2018): 213-233.
- Mohammed Alqahtani and Robin Braun (2021), "Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review", Journal of Information Assurance & Cybersecurity, Vol. 2021 (2021), Article ID 666987, DOI: 10.5171/2021.666987
- R. Pal, L. Golubchik, K. Psounis and P. Hui, "Will cyber-insurance improve network security? A market analysis," IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2014, pp. 235-243, doi: 10.1109/INFOCOM.2014.6847944.
- Sergeja Slapničar, Tina Vuko, Marko Čular, Matej Drašček, Effectiveness of cybersecurity audit, International Journal of Accounting Information Systems, Volume 44, 2022, 100548, ISSN 1467-0895,

https://doi.org/10.1016/j.accinf.2021.100548, https://www.sciencedirect.com/science/article/pii/S1467089521000506.

- Simonova, A. (2020). An analysis of factors influencing national institute of standards and technology cybersecurity framework adoption in financial services: A correlational study (Order No. 27998512). Available from ProQuest Dissertations & Theses A&I; Publicly Available Content Database. (2418554226). Retrieved from https://ezp.lib.cam.ac.uk/login?url=https://www.proquest.com/dissertations-theses/analysis-factors-influencing-national-institute/docview/2418554226/se-2.

- Stewart, Harrison. "Why ISO27001 Certified Organizations Still Experience Data Leakage?." Journal of Digital Information Management 20.3 (2022): 91.

C.2 Web

- A/S, Neupart. ISO 27001 - The Standard for Information Security, https://www.neupart.com/resources/iso-27001#:~:text=ISO%2027001%20was%20released%20as,and%20then%20again%20in%202022.Accessed20July2023.

- Ackerman, Spencer. "5 Nuclear Sites That Could Launch War with Iran." Wired, 21 May 2012, https://www.wired.com/2012/05/iran-nuclear-sites/.

- Albrycht, Elizabeth. "11 Jan Summary of Pending NIST Cybersecurity Framework (CSF) Changes in Version 1.1 Draft 2." Criterion Systems, 11 Jan. 2018, https://www.criterion-sys.com/summary-of-pending-nist-cybersecurity-framework-csf-changes-in-version-1-1-draft-2/.

- Anderson, Kevin. "US Analysis of Google Attack Code Finds Chinese Fingerprints." The Guardian, 20 Jan. 2010, https://www.theguardian.com/technology/blog/2010/jan/20/google-china.

- Banga, Gaurav. "Council Post: How to Ensure Your NIST Cybersecurity Framework Implementation Isn't Too Little, Too Late." Forbes, 3 Nov. 2020, www.forbes.com/sites/forbestechcouncil/2020/11/04/how-to-ensure-your-nist-cybersecurity-framework-implementation-isnt-too-little-too-late/.

- CATHY BUSSEWITZ, BEN FINLEY and TOM FOREMAN. "Colonial Pipeline Restarts Operations Days after Major Hack." WPTV News Channel 5 West Palm, 12 May 2021, https://www.wptv.com/news/national/colonial-pipeline-restarts-operations-days-after-major-hack.

- Corfield, Gareth. "UK and Chums Call Out Chinese MSS for Hafnium Microsoft Exchange Server Attacks." The Register® - Biting the Hand That Feeds IT, 19 July 2021, https://www.theregister.com/2021/07/19/hafnium_china_state_security/.
- Edwards, Max. "ISO 27002:2022 Changes, Updates and Comparison." ISMS.Online, 1 Mar. 2022, https://www.isms.online/iso-27002/iso-27002-revisions-updates-comparison/#:~:text=The%202022%20version%20includes%2024,element%20in%20the%202022%20version.
- Gazula, Mohan Buvana. Cyber Warfare Conflict Analysis and Case Studies. Diss. Massachusetts Institute of Technology, 2017. https://dspace.mit.edu/handle/1721.1/112518.
- Getting Started. NIST. (2023, April 21). https://www.nist.gov/cyberframework/getting-started.
- Goodin, Dan. "More than 20GB of Intel Source Code and Proprietary Data Dumped Online." Ars Technica, 6 Aug. 2020, https://www.arstechnica.com/information-technology/2020/08/intel-is-investigating-the-leak-of-20gb-of-its-source-code-and-private-data/.
- ISO, Org. "ISO/IEC 27001 Standard – Information Security Management Systems (ISMS)." ISO, 13 Apr. 2023, https://www.iso.org/standard/27001.
- Johns, Emma, and Maddy Ell. "Cyber Security Breaches Survey 2023." GOV.UK, 19 Apr. 2023, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.
- Kelly, Stephanie, and Jessica Resnick-Ault. "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators." Reuters, 9 June 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.
- Kerner, Sean Michael. "Colonial Pipeline Hack Explained: Everything You Need to Know." WhatIs.Com, 26 Apr. 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=What%20was%20the%20root%20cause,Homeland%20Security%20on%20June%208.
- Kimmerle, Kris. "Quick Analysis of NIST CSF 2.0." LinkedIn, 8 May 2023, https://www.linkedin.com/pulse/quick-analysis-nist-csf-20-draft-kris-kimmerle/.
- Lee, Timothy B. "The Devastating Hack of the Federal Office of Personnel Management, Explained." Vox, 27 June 2015, https://www.vox.com/2015/6/27/8854765/opm-hack-explained.

- Levine, Mike. "22 Million Affected by OPM Hack, Officials Say - University of Central ..." ABC News, 5 July 2015, https://www.security.research.ucf.edu/Documents/News/22%20Million%20Affected%20by%20OPM%20Hack.pdf.

- Lineman, David. "ISO 27002:2013 Change Summary Heatmap." Information Shield, 23 May 2022, https://www.informationshield.com/2013/11/15/iso-270022013-change-summary-heatmap/.

- Lubbert, Adam. "ISO 27001:2013 vs ISO 27001:2022: CSA." ISO 27001:2013 vs ISO 27001:2022 — CSA, 2 Oct. 2023, https://www.cloudsecurityalliance.org/blog/2023/02/10/what-s-the-difference-between-iso-27001-2013-and-iso-27001-2022/.

- Mandiant. "Top Trends in Cyber Security: Cyber Attacks Trends: M-Trends." Mandiant, 18 Apr. 2023, https://www.mandiant.com/m-trends.

- Mar 21, 2023. "2023 Unit 42 Ransomware and Extortion Report." Palo Alto Networks, 21 Mar. 2023, https://www.paloaltonetworks.com/resources/research/2023-unit42-ransomware-extortion-report#.

- Merry, Anthony. "Kaseya VSA Supply Chain Ransomware Attack." Sophos News, 8 Sept. 2021, https://www.news.sophos.com/en-us/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack/.

- Nair, Prajeet, and Ron Ross. "Colonial Pipeline May Have to Pay Fine of Nearly $1 Million." Bank Information Security, 10 May 2022, https://www.bankinfosecurity.com/colonial-pipeline-may-have-to-pay-nearly-1-million-fine-a-19050#:~:text=%22At%20the%20time%20of%20the,demonstrate%20compliance%2C%22%20it%20adds.

- Newman, John, and Amy Ritchie. "Equifax Data Breach Settlement." Federal Trade Commission, 20 Dec. 2022, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement#FAQ7.

- Ng, Alfred. "How the Equifax Hack Happened, and What Still Needs to Be Done." CNET, 7 Sept. 2018, https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

- NIST. "Discussion Draft of the NIST Cybersecurity Framework 2.0 Core." Discussion Draft of Updates to NIST CSF 1.1 Core, Apr. 2023. https://www.nist.gov/system/files/documents/2023/04/

24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%2042023%20final.pdf.

- Nyman, Mike. "New SOC 2 Report Framework Addresses Emerging Risks." 2018: Articles: Resources: CLA (CliftonLarsonAllen), 15 May 2018, https://www.claconnect.com/en/resources/articles/2018/new-soc-report-framework-addresses-emerging-risks.

- Obama, Barack H. "Executive Order – Improving Critical Infrastructure Cybersecurity." National Archives and Records Administration, 12 Feb. 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

- Saleem, Hamza. "United States Office of Personnel Management (OPM) Data Breach, 2014 ..." ResearchGate.Net, Oct. 2020, www.researchgate.net/figure/United-States-Office-of-Personnel-Management-OPM-Data-Breach-2014_fig2_346937548.

- Sanders, James. "Spectre and Meltdown Explained: A Comprehensive Guide for Professionals." TechRepublic, 15 May 2019, https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/.

- Sean Gallagher; Jun 16, 2015 7:22 pm UTC. "Encryption 'Would Not Have Helped' at OPM, Says DHS Official." Ars Technica, 16 June 2015, https://www.arstechnica.com/information-technology/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/.

- Varma, Rohit. "McAfee Labs: Combating Aurora." (2010). https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Combating%20Threats%20-%20Operation%20Aurora.pdf.

- Wadhwani, Sumeet. "Is Revil's Latest Exploit against Kaseya One of the Biggest Ransomware Attacks Ever?" Spiceworks, 23 July 2021, https://www.spiceworks.com/it-security/vulnerability-management/news/is-revils-latest-exploit-against-kaseya-one-of-the-biggest-ransomware-attacks-ever/.

- "2017 Trust Services Criteria (with Revised Points of Focus – 2022)." AICPA, https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022. Accessed 1 Aug. 2023.

- "2022 INTERNET Crime Report - Internet Crime Complaint Center (IC3)." IC3 2022 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Accessed 25 July 2023.
- "August 2018 Data Protection - Elizabeth Warren." Government Accountability Office (GAO), Aug. 2018, https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf.
- "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities: CISA." Cybersecurity and Infrastructure Security Agency CISA, 13 June 2023, https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities.
- "Chinese Hackers Charged in Equifax Breach." FBI, 10 Feb. 2020, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020.
- "Cybersecurity Resource Center: OPM Breach." U.S. Office of Personnel Management, https://www.opm.gov/about-us/our-people-organization/office-of-the-general-counsel/cybersecurity-resource-center/.Accessed30July2023.
- "Cybersecurity Trends: Looking Over the Horizon." McKinsey & Company, 10 Mar. 2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon.
- "Discussion Draft of the NIST Cybersecurity Framework 2.0 Core." NIST, https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf. Accessed 1 Aug. 2023.
- "Earning Your Trust." Kaseya, 8 May 2023, https://www.kaseya.com/trust-center/earning-your-trust/#:~:text=ISO%2027001,to%20the%20ISO%2027001%20standard.
- "Equifax Held ISO 27001 Certification at Time of Massive System Hack." Oxebridge Quality Resources International, 22 Sept. 2018, https://www.oxebridge.com/emma/equifax-held-iso-27001-certification-at-time-of-massive-system-hack/.
- "Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy." The White House, 2 Mar. 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

- "FY22 Risk and Vulnerability Assessments (RVA) Results - CISA." CISA Risk Vulnerability Assessment Center, July 2023, https://www.cisa.gov/sites/default/files/2023-07/FY22%20RVA%20Infographic_508c.pdf.
- "Incident Overview & Technical Details – Kaseya." Kaseya Helpdesk, https://www.helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details.Accessed30July2023.
- "Intel Sourcing and Manufacturing Security Practices Overview." Intel, www.intel.com/content/www/us/en/security/security-practices/sourcing-manufacturing-security.html.Accessed29July2023.
- "NIST CVD." NVD, https://www.nvd.nist.gov/vuln/data-feeds. Accessed 1 Aug. 2023.
- "NIST Releases Version 1.1 of Its Popular Cybersecurity Framework." NIST, 16 Apr. 2018, www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.
- "Panaseer 2022 Security Leaders Peer Report." Panaseer, 11 July 2023, https://panaseer.com/reports-papers/report/2022-security-leaders-peer-report/.
- "Press Release." Security and Exchange Commission (SEC), 26 July 2023, https://www.sec.gov/news/press-release/2023-139.
- "Security Orchestration Automation and Response (SOAR) Playbook." Rapid7, www.rapid7.com/info/security-orchestration-and-automation-playbook/. Accessed 25 July 2023.
- "Selecting a Protective DNS Service - U.S. Department of Defense." Cyber Security Information, CISA, May 2021, media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_PROTECTIVE%20DNS_UO0117652-21.PDF.
- "SOC 2 and ISAE 3000." SOC2, https://www.soc2.co.uk/soc-2. Accessed 21 July 2023.
- "Stellar Cyber's AI-Driven Incident Correlation Increases Attack Detection Efficiency." Help Net Security, 28 July 2021, https://www.helpnetsecurity.com/2021/07/28/stellar-cyber-incident-correlation/.
- "The ISO Survey." ISO, 22 Feb. 2023, https://www.iso.org/the-iso-survey.html.

- "Uses and Benefits of the Framework." NIST, 16 Mar. 2023, www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework.

C.3 Blogs

- Boeckmann, Chad. "Changes between NIST CSF 1.0 to NIST CSF 1.1 - Trustmapp: Cybersecurity Performance Management." TrustMAPP, 13 June 2018, https://www.trustmapp.com/changes-between-nist-csf-1-0-to-nist-csf-1-1/.

- Card, Daniel. "ISO27001 Thoughts." Twitter, 15 July 2023, https://twitter.com/UK_Daniel_Card/status/1680248995317182467.

- Gupta, Amartya. "Ransomware Attack – A Nightmare for Any IT Team." Motadata, 16 May 2017, www.motadata.com/blog/wannacry-ransomware-attack/.

- Irwin, Luke. "ISO 27001 VS SOC 2 Certification: What's the Difference?" IT Governance Blog En, 23 Jan. 2023, https://www.itgovernance.eu/blog/en/iso-27001-vs-soc-2-certification-whats-the-difference.

- Kosutic, Dejan. "What Are the 11 New Security Controls in ISO 27001:2022?" 27001Academy, 20 Jan. 2023, https://www.advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/.

- Kutscher, Jurgen. "M-Trends 2023: Cybersecurity Insights From the Frontlines." Mandiant, 18 Apr. 2023, https://www.mandiant.com/resources/blog/m-trends-2023.

- Step-by-Step Guide SOC 2, Apr. 2022, https://risklane.com/sites/default/files/2022-05/Step-by-step%20Guide%20for%20SOC%202%20Compliance.pdf.

- Viggiani, Fabio. "The Solarwinds Orion Sunburst Supply-Chain Attack." Truesec, 16 Dec. 2020, https://www.truesec.com/hub/blog/the-solarwinds-orion-sunburst-supply-chain-attack.

- "2023 Data Breach Investigations Report (DBIR)." Verizon Business, https://www.verizon.com/business/resources/reports/dbir/. Accessed 25 July 2023.

- "Regex Support." CHAOSSEARCH Knowledge Center, https://docs.chaossearch.io/docs/regex-support.Accessed25July2023.

THIS PAGE LEFT INTENTIONALLY BLANK