The Application of Information Privacy Frameworks in Cybersecurity

Dale Dunn

INTRODUCTION

The frequency of cyberattacks is increasing exponentially, with human-driven ransomware attacks more than doubling in number between September 2022 and June 2023 alone.[1] In a vast majority of attacks, threat actors seek to penetrate legitimate accounts of their target's employees or the accounts of their target's third-party service provider's employees.[2] In the remaining instances, threat actors exploit existing vulnerabilities to penetrate their target's systems.[3] Combatting these attacks requires a holistic, whole-of-society approach.

Current technology and security norms leave room for improvement. The Cybersecurity and Infrastructure Security Agency (CISA) describes current technology products as generally being vulnerable by design ("VbD").[4] To help companies produce secure products instead, CISA, in combination with its partners, has proposed the Secure by Design ("SBD") framework.[5] However, SBD will not be sufficient on its own to prevent threat actors from succeeding. The quantity and availability of personal information available today enables threat actors to efficiently bypass security measures.

The Fair Information Practice Principles ("FIPPs") and the Privacy by Design ("PBD") framework should be implemented in addition to SBD to reduce both the likelihood and the

---

[1] MICROSOFT THREAT INTEL., MICROSOFT DIGITAL DEFENSE REPORT 17 (2023) ("[O]rganizations faced an increased rate of ransomeware attacks . . . up more than 200 percent since September 2022.").
[2] *Id.* at 16 ("[T]hese are the top threats identified by Microsoft Defender Experts this year: 1) [s]uccessful identity attacks; 2) [r]ansomware encounters; 3) [t]argeted phishing attempts leading to device or user compromise; [and] 4) [b]usiness email compromise.").
[3] *Id.* at 17 ("Among vulnerable external facing applications, cybercriminals exploited vulnerabilities . . . . ").
[4] *See* CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, SECURE BY DESIGN 4 (2nd ed. 2023) (arguing that technology manufacturers are introducing insecure products into the market that have inherent vulnerabilities, increasing their risk of penetration by cyberattacks).
[5] *Id.*

potential harm of successful cybersecurity attacks. The FIPPs are procedures for handling data that mitigate the risk of misuse.[6] PBD is a supplementary method of mitigating the potential harm that can result from data in a system or product.[7] While both the FIPPs and PBD were developed for use with personal information, they can and should apply beyond that specific context as a way of thinking about all data used and protected by information systems.

This paper is arranged in five sections. The first section describes the requirement of reasonable security. The second section then explains the Secure by Design framework. Section three, the FIPPs and PBD. Section four provides a case study in which social engineering is utilized by a threat actor to conduct cyberattacks. Finally, section five recommends measures companies and other organizations should take to implement the SBD, FIPPs, and the PBD. In sum, this paper will show information privacy principles and methodologies that should be implemented to reduce the risk of cybersecurity attacks.

1. REASONABLE SECURITY

Entities are generally required by most laws and regulatory regimes to maintain reasonable cybersecurity programs that are proportionate to their circumstances. Cybersecurity is fundamentally, a matter of risk management.[8] A reasonable cybersecurity program must balance security and convenience in relation to the degree of risk it is willing to accept. Unfortunately, increased security comes at the expense of decreased convenience.[9] The greater the degree of

---

[6] Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY FORUM (Dec. 19, 2007) https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ ("Fair Information Practices are a set of principles and practices that describe . . . an . . . approach [of] information handling, storage, management, and flows with a view toward maintaining fairness, privacy, and security . . . .").
[7] *See* ANN CAVOUKIAN, PRIVACY BY DESIGN THE 7 FOUNDATION PRINCIPLES: IMPLEMENTATION AND MAPPING OF FAIR INFORMATION PRACTICES 1-2 (arguing the benefits of innovation must be balanced against the protection of personal data and that PBD "must be incorporated into networked data systems and technologies, by default").
[8] JAMES X. DEMPSEY, CYBERSECURITY LAW FUNDAMENTALS 78 (Joni L. McNeal ed., 2021) ("Cybersecurity . . . is a matter of risk reduction.").
[9] *See* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED 69-70 (David McBride & Holly Mitchell eds., 2022) ("People are careless because good security is often cumbersome and inconvenient.").

increased security, the greater the degree of decreased convenience, and the more likely people are to circumvent or not use the security measure.[10] Good cybersecurity is about making your system as secure as possible, but not making it so secure that people will not adhere to it.[11] Humans are the primary flaw in most cybersecurity programs.[12] Information privacy, as part of a reasonable cybersecurity program, can help mitigate the impact of humans on the system and the potential consequences of their role in data breaches by reducing the amount of data entities maintain.[13]

Companies must assess whether their cybersecurity programs are reasonable holistically, instead of just through a technical lens.[14] Every byte of data a company uses or possesses creates risk.[15] Every person, inside or out of a company, who has access to that company's data, presents a risk.[16] Every function an organization does that involves data, increases the risk to the organization.[17] It is unreasonable for an entity to not consider the cybersecurity risk associated with the data it collects or uses and subsequently not implement safeguards or procedures to reduce such risk.[18]

Because business models have become dependent on mass data collection and processing, they are likely to push back against any suggestion that they minimize the amount of data they

---

[10] *Id.* at 72 ("One of the basic tendencies of human nature is that the more inconvenient something is, the less people will do it.").
[11] *Id.* at 74 (arguing that good data security is the art of determining how much risk an entity will accept in relation to the degree of security it requires).
[12] *Id.* at 159 ("In most data breaches, human error has played a significant role in enabling or failing to prevent the breach.").
[13] *See id.* at 68-69.
[14] MICROSOFT THREAT INTEL., *supra* note 1 at 24 ("Cybersecurity can no longer be seen as a technical problem, for greater resilience it must be seen as an organization risk… and managed accordingly.").
[15] SOLOVE & HARTZOG, *supra* note 9, at 69 ("Every time data is stored, there's a security risk.").
[16] *Id.* ("Every time access to data is granted, there's a security risk.").
[17] *Id.* ("Every time data is transferred, there's a security risk. Anything involving the Internet is risky. Email is risky. Sharing files is risky.").
[18] DEMPSEY, *supra* note 8, at 79 (describing reasonableness as the standard used in determining the threshold of cybersecurity entities are required to maintain).

collect and use.[19] This, however, would give too much leeway to organizations. Companies should employ data minimization to reduce their exposure to risk and exposure to others.[20]

Between November 2022 and June 2023, Microsoft observed a 100% increase in data exfiltration instances.[21] Data harvested during exfiltration instances is used for subsequent penetration attempts, not just for ransomware.[22] The data that companies maintain and use does not just present a risk to themselves; it presents a risk to the broader cybersecurity landscape.

In 2022 the Office of the Director of National Intelligence (ODNI) issued its report on Commercially Available Information (CAI).[23] The ODNI defines CAI as "information that is available commercially, through a commercial transaction with another party."[24] The ODNI further defines CAI as:

> Any information that is of a type customarily made available or obtainable and sold, leased, or licensed to the general public or to non-governmental entities for purposes other than governmental purposes. [CAI] also includes information for exclusive government use, knowingly and voluntarily provided by, procured from, or made accessible by corporate entities at the request of a government entity, or on their own initiative.[25]

This is not data that the government is collecting on citizens through its own operations. This is data that businesses and other organizations have already collected on their customers. These entities then sell the data they collected to data brokers, who then sell it on to their customers.[26] To

---

[19] MARK SETTLE, PRIVACY BY DESIGN: FROM PRINCIPLES TO REQUIREMENT 16 (2021) (arguing that because organizations have become dependent on insights derived from data about their customers data minimization has become unrealistic).
[20] *Id.* at 17 ("Data that is not absolutely required should be generalized, redacted, anonymized or eliminated altogether. Data that is not in active use should be archived or destroyed.").
[21] MICROSOFT THREAT INTEL., *supra* note 1, at 22.
[22] *Id.* ("Not all data theft is associated with ransomware; it can also be part of credential harvesting or nation-state espionage.").
[23] OFF. OF THE DIR. OF NAT'L INTEL. SENIOR ADVISORY GRP., PANEL ON COMMERCIALLY AVAILABLE INFORMATION (2022).
[24] *Id.* at 4.
[25] *Id.*
[26] *Id.*

help the reader understand the extent of the CAI held by data brokers, the ODNI provided four examples. Two of their examples that are particularly demonstrative are "LexisNexis offers more than '84B records from 10,000+ sources, including alternative data that helps surface more the 63M unbanked/underbanked U.S. adults,'" and "PeekYou 'collects and combines scattered content from the social sites, news sources, homepages, and blog platforms to present comprehensive online identities.'"[27]

Of particular relevance to the field of cybersecurity is what the ODNI identifies as counter-intelligence risks, the ability of foreign actors to use CAI for intelligence purposes.[28] The same data that criminal organizations may use to target government officials may also be used to build profiles on employees and customers and subsequently target them to facilitate access.[29] This opportunity only exists because of the magnitude of the data collected in the first place.

Organizations should pseudonymize data where possible, and ideally, anonymize that data.[30] Pseudonymous data consists of personal data which has been processed in a way that the personal data can longer be attributed to a specific individual without the use of additional information.[31] When an organization pseudonymizes data, it must keep separate the additional information that would allow the pseudonymous data to be attributed to a person.[32] Ideally, anonymous data consists of personal data that has been processed in a way that the data can no longer "be related back to a given individual."[33] Unfortunately, when data is anonymized, it is still

---

[27] *Id.* at 4.
[28] *Id.* at 11.
[29] JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS 11 (2021).
[30] LUJO BAUER ET AL., AN INTRODUCTION TO PRIV. FOR TECH. PRO. 215 (Travis D. Breaux ed., 2020)
[31] *Pseudonymous Data*, INT'L ASS'N OF PRIV. PRO, https://iapp.org/resources/glossary (last visited Dec. 12, 2023).
[32] *Id.*
[33] *Id.* at *Anonymous Information*.

possible to identify data subjects. Anonymized data can be de-anonymized through the use of additional information.[34] Ultimately, there is no substitute for not collecting data in the first place.

2. SECURE BY DESIGN

Secure by design consists of three core principles.[35] The three principles are: take ownership of customer security outcomes, embrace radical transparency and accountability, and build organizational structure and leadership to achieve these goals.[36] SBD also incorporates the concept of secure by default.[37] Secure by default is the idea that products are shipped from manufacturers in a state that will be secure from the moment of first use.[38]

2.1 Take Ownership of Customer Security Outcomes

The first principle of SBD, "take ownership of customer security outcomes," establishes that the entity in the best position to improve security should be primarily responsible for doing so.[39] That will typically mean software and hardware manufacturers,[40] and notably, not their customers. Customers are poorly positioned to address their own security for each of their products. Manufacturers are comparatively much better situated.[41] SBD recommends that manufacturers should focus on application hardening, features, and default settings.[42]

Application hardening seeks to infuse products with security throughout their systems, thereby foreclosing known, natural vulnerabilities.[43] Rolling out comprehensive solutions at the

---

[34] OFF. OF THE DIR. OF NAT'L INTEL. SENIOR ADVISORY GRP., *supra* note 23, at 8 ("Although CAI may be 'anonymized,' it is often possible (using other CAI) to deanonymize and identify individuals, including U.S. persons.").
[35] *See* CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 4, at 10.
[36] *Id.*
[37] *Id.* at 4 ("The term 'secure by design' encompasses both secure design and secure by default.").
[38] *Id.* at 9 ("'Secure by default' means products are resilient against prevalent exploitation techniques out of the box without added charge.").
[39] *Id.* at 11.
[40] *See id.* at 10.
[41] *See id.* at 10 ("The burden of security should not fall solely on the customer").
[42] *Id.* at 11 (providing examples of features such as transport layer security, single sign on, and multifactor authentication and suggesting that out of the box settings be set to their most secure configuration).
[43] *Id.* .

earliest point in the stream, when they are being manufactured, increases the likelihood of the hardening being effective.[44] Examples of hardening techniques are: (1) parameterized queries; (2) memory safe programming language; (3) software development life cycle (SDLC) management; and (4) hardware-backed cryptographic key management.[45]

Failing to take these measures initially, or where vulnerabilities are found, results in customers having to plug the holes in their software by patching. Manufacturers will ship patches to various problems as they arise, rather than eliminating an entire class of vulnerability entirely.[46]

The Equifax breach was a prime example of the impact manufacturers shipping VbD products can have on their customers. Equifax is a national consumer reporting agency.[47] On March 8, 2017, the United States Computer Emergency Readiness Team (US-CERT) notified Equifax, a national consumer reporting agency, of the Apache Struts vulnerability, CVE-2017-5638, which allowed threat actors to execute code remotely.[48] Equifax's security team notified its employees on March 9, 2017 via e-mail that if they oversaw a program that ran Apache Struts, they needed to install the provided patch within 48 hours.[49] Equifax did not discover they had not patched the vulnerability within the ACIS Dispute Portal until approximately July 30, 2017.[50] Because of the vulnerability, attackers were able to steal "147 million names and dates of birth, 145.5 million SSNs, 99 million physical addresses, 20.3 million telephone numbers, 17.6 million e-mail addresses, and 209,000 payment card numbers and expiration dates."[51] Had Java focused on shipping secure software and addressed this vulnerability before providing Apache Struts to

---

[44] *See id.* at 12.
[45] *Id.* at 11.
[46] *Id.* at 12.
[47] Complaint for Permanent Injunction and Other Relief at 3, Federal Trade Commission v. Equifax Inc., N.D.Ga (2019) (No. 1:19-cv-03297-TWT), 2019 WL 3287211.
[48] *Id.*
[49] *Id.*
[50] *Id.* at 7.
[51] *Id.* at 8.

consumers, this vulnerability would not have existed to be exploited. If Equifax had not collected this data, the data would not have been breached.

Apache Struts and other products that have configurable settings should be shipped in their most secure setting as the default.[52] Shipping products with features that are not set to their safest setting can increase customers' attack surfaces.[53] Shipping products with settings that are secure by default reduces the risk that stems from the different levels of familiarity manufacturers' clients may have with cybersecurity.[54] Secure by default practices can help manufacturers achieve the goal of producing secure products.[55]

CISA recommends manufacturers use the following SBD practices in pursuit of the first principle: (1) eliminate default passwords; (2) conduct field tests; (3) reduce hardening guide size; (4) actively discourage use of unsafe legacy features; (5) implement attention grabbing alerts; and (6) create secure configuration templates.[56] These practices focus on making security easier and more natural for customers. Manufacturers consistently ship products with default passwords that customers do not bother to change when they set up their product. Once threat actors know those default passwords, they are able to use them in accessing a majority of those devices.[57] Eliminating default passwords should likely reduce the efficiency of threat actors' operations. They should no longer be able to penetrate a myriad of targets, having only acquired one piece of information. Whether an individual consumer or business, customers can not be relied on to maintain reasonably cybersecurity.

---

[52] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 4, at 12.
[53] *Id.* at 12-13.
[54] *Id.* at 13.
[55] *Id.*
[56] *Id.* at 14-16.
[57] *Id.* at 15 ("Default passwords continue to be implicated as the cause of many attacks every year.").

Where customers do not perceive a significant enough risk to warrant the effort, they will not keep their cybersecurity program up to date.[58] CISA recommends manufacturers actively discourage the use of unsafe legacy features.[59] However, if manufacturers stop supporting products without consideration for their customers, they may face backlash.[60] Customers will likely resent such efforts if the cost-benefit analysis does not make sense for their purposes.

2.2. Embrace Radical Transparency and Accountability

The second principle, "embrace radical transparency and accountability," advocates for manufacturers to communicate their process for software development.[61] Such transparency should help manufacturers learn from each other and help customers choose products with an awareness of the security they provide.[62] CISA has several recommendations for companies to achieve such transparency and accountability. First, CISA recommends that manufacturers employ the pertinent SBD practices of publishing aggregate security-relevant statistics and trends, including statistics on patching and unused privileges.[63] Second, CISA recommends that manufacturers follow several secure development practices, such as establishing internal security controls.[64] And third, CISA recommend that companies publicly name a SBD senior executive sponsor and publish SBD and memory-safety roadmaps.[65]

---

[58] *Id.* at 16 ("A significant number of customers have demonstrated that they will not keep their systems current with modern network, identity, and other critical security features").
[59] *Id.* ("Software manufacturers should aggressively nudge customers along upgrade paths that reduce customer risk.").
[60] *But see id.* (arguing manufacturers can convince customers to happily upgrade their security more often and quickly by making upgrades as seamless as possible, explaining why they should upgrade, and deprecating unsafe features).
[61] *See id.* at 16 (observing manufacturers rarely publish their processes for developing and maintaining their software or how they mature their programs).
[62] *Id.* at 20-21 (arguing transparency will move the software industry forward at an exponentially faster rate by sharing methods between manufacturers and providing customers with information on the security of products, thereby incentivizing manufacturers through capitalism).
[63] *Id.* at 22.
[64] *Id.*, at 23.
[65] *Id.* at 25.

Placing ownership of the SBD program on a senior executive should prioritize SBD in a way that should enable it to move from being merely a technical concern to part of the business' ethos.[66] Without a senior executive as a sponsor, the SBD program would likely lack the force to enact meaningful change. As part of his responsibilities, the senior executive should oversee the development and adoption of the SBD program.

The SBD program should include a "secure by design roadmap." The details of a roadmap should provide the company and its employees with the direction they need to make meaningful progress.[67] Furthermore, a roadmap should also detail to others, and the manufacturer itself, the measures taken to make its products more secure.[68] One such sub-component should be the production of a "memory-safety roadmap."[69]

Memory-safety vulnerabilities are one of the largest classes of vulnerabilities.[70] In 2019, the Microsoft Security Response Center (MSRC) noted, "70% of the vulnerabilities Microsoft assigns a CVE [common vulnerability and exposure] each year continue to be memory safety issues."[71] The Chromium Project also stated that "around 70% of our serious security bugs are memory safety problems."[72] Also in support of this proposition, Mozilla reported that of the 34 critical/high bugs they identified, 32 possessed severe, memory-related security problems.[73]

---

[66] *Id.* (arguing, that naming a top business executive to oversee SBD would turn it into a whole-of-business concern, instead of being relegated to the technical teams).
[67] *See id.*
[68] *Id.*
[69] *Id.*
[70] Bob Lord, *The Urgent Need for Memory Safety in Software Products*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY (Dec. 6, 2023), https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products.
[71] *A Proactive Approach to More Secure Code*, MICROSOFT SEC. RESPONSE CTR. (Jul. 6, 2019), https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/.
[72] *Memory Safety*, THE CHROMIUM PROJECTS, https://www.chromium.org/Home/chromium-security/memory-safety/ (last visited Dec. 10, 2023).
[73] Diane Hosfelt, *Implications of Rewriting a Browser Component in Rust*, MOZILLA HACKS (Feb. 28, 2019), https://hacks.mozilla.org/2019/02/rewriting-a-browser-component-in-rust/.

Implementing a memory-safety roadmap should assist manufacturers in eliminating one of the largest threats to customer safety wholesale.

2.3. Lead From the Top

The third principle, "Lead from the Top," may be the most important principle of SBD and have the greatest impact overall on the security of a manufacturer's products.[74] The "Tone at the Top," a compliance and risk management concept, determines the quality of a manufacturer's product.[75] Manufacturers must demonstrate to their designers and engineers from the outset that the production of secure products is a priority by allocating the necessary resources to SBD.[76] Security must be approached holistically, and part of that is making the business decision about what data is necessary and how that data will be managed.[77]

CISA recommends that manufacturers take several steps to fulfill this principle.[78] Most significant among those steps are the creation of meaningful internal incentives, a secure by design council, and customer councils.[79] Employees prioritize the metrics their employer objectively supports through action.[80] Manufacturers should incentivize employees by rewarding them for work that supports the SBD philosophy.[81] A secure by design council should facilitate the integration of SBD through an organization, from the bottom to the top.[82] Forming a council and embedding its representatives in the various divisions and units allows those representatives to

---

[74] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 4, at 26 ("Only when senior leaders make security a business priority, creating internal incentives and fostering an across-the-board culture to make security a design requirement, will they achieve the best results.").
[75] *Id.*("How a company establishes its vision, mission, values, and culture will affect the products.").
[76] *Id.* (arguing manufacturers have to invest the necessary resources to ensure SBD is central to their business model).
[77] *Id.* ("[E]nsur[ing] that software security is a core business priority from the beginning will reduce the long-term costs of addressing software defects-and in turn, lower the national security risks.").
[78] *Id.* at 27.
[79] *Id.*
[80] See *id.*
[81] *Id.*(arguing manufacturers should reward employees that improve customer security in a way that is equal to reward systems for other behaviors the company values).
[82] *See id.*

receive bottom-up refinement.[83] Manufacturers can combine the effects of these efforts with the benefits they would receive by establishing "customer councils."[84] Such councils, where used in the industry, are designed to represent a broad swatch of the manufacturer's customers.[85] The diversity of these councils will help manufacturers understand how the different aspects of their customers impact the effectiveness of their product, allowing them to trim the excess from their products that might otherwise create unnecessary attack vectors.[86]

2.4 Secure by Design and Default Tactics

Alongside and in support of the three SBD principles, CISA and its collaborators advocate the use of the following best practices which they have separated into two categories, Secure by Design Tactics and Secure by Default Tactics.[87] The secure by design tactics, meant to be incorporated into a manufacturers development process, includes: (1) memory safe programming languages; (2) secure hardware foundation; (3) secure software components; (4) web template frameworks; (5) parameterized queries; (6) static and dynamic application security testing; (7) code review; (8) software bill of materials (SBOM); (9) vulnerability disclosure programs; (10) CVE completeness; (11) defense-in-depth; and (12) satisfy cybersecurity performance goals (CPGs).[88] The secure by default tactics, meant to guide manufacturers in how their products should be configured once shipped, includes: (1) eliminate default passwords; (2) mandate multifactor authentication (MFA) for privileged users; (3) single sign-on (SSO); (4) secure logging; (5) software authorization profile; (6) forward-looking security over backwards compatibility; (7)

---

[83] *Id*. ("By including both centralized and distributed members, these groups work to improve quality against top level goals while receiving telemetry from deep in the organization.").
[84] *Id*. (arguing customer councils provide useful feedback about the successes and challenges they had using the manufacturer's products).
[85] *Id.* (observing customer councils normally consist of customers from different regions and industries and of different sizes).
[86] *See id.*
[87] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 4, at 28-31.
[88] *Id.*

track and reduce "hardening guide" size; and (8) consider the user experience consequences of security settings.[89]

The use of secure by design principles and tactics would go a long way toward creating a more secure digital environment. To be successful in their efforts, manufacturers will need to tailor their products to address the risk presented by relevant threat-models and hold themselves accountable for creating products that meet that challenge.[90] While SBD should largely address threat issues such as actors that use software vulnerabilities to successfully penetrate an organization's shell or integrated software, it does not adequately address social engineering [issues?], the other method of access discussed at the beginning. To do that, organizations will also need to view the FIPPs and PBD as more than a framework for just protecting their customers' privacy.

3. The FIPPs & PRIVACY BY DESIGN

PBD builds on top of the foundations provided by the FIPPs to establish a framework for embedding privacy into every step of product or program design.[91] The FIPPs are a set of practices used when assessing products, programs, or systems for their impact on personal data.[92] The nine FIPPs are (1) access and amendment; (2) accountability; (3) authority; (4) minimization; (5) quality and integrity; (6) individual participation; (7) purpose specification and use limitation; (8) security; and (9) transparency.[93] Accountability, authority, minimization, and purpose specification and use limitation are the practices most relevant to cybersecurity.

---

[89] *Id.* at 30-31.
[90] *See id.* at 11 (recommending manufacturers emphasize the importance of SBD to their business success within their organization and use tailored threat models to determine the most important features that should be prioritized in allocating resources).
[91] CAVOUKIAN, *supra* note 7, at 1-2 (arguing PBD affirms and incorporates the FIPPs to provide a method for embedding privacy in every aspect of life).
[92] *Fair Information Practice Principles*, FED. PRIV. COUNCIL, https://www.fpc.gov/resources/fipps/ (last visited Dec. 12, 2023).
[93] *Id.*

PBD was meant to be a leap forward~~,~~, in the protection of personal data.[94] PBD consists of seven principles: (1) Proactive, Not Reactive; Preventative, Not Remedial; (2) Privacy as the Default; (3) Privacy Embedded Into Design; (4) Full Functionality (Positive Sum, Not Zero Sum); (5) End-to-End Security (Lifecycle Protection); (6) Visibility and Transparency; and (7) Respect for User Privacy.[95]

The first principle, proactive not reactive; preventative not remedial is meant to encourage organizations, before beginning development, to consider what harms might occur and how to prevent them.[96] Organizations are generally required to provide notice when there is a breach of personal information or when a cyberattack would be of material concern. Many regulatory regimes provide an exception to notification where data was encrypted or where personal information was not breached. Organizations should recognize the inherent value of avoiding the consequences of a cyberattack or breach in the first place and implement steps to reduce this risk.[97]

To achieve this, organizations must implement data privacy frameworks that allow them to identify risks to information privacy and develop solutions to resolve them before the risk is realized.[98] For example, they could encrypt all data at rest and in transit, as well as segregate categories of data that might otherwise be personal information where they compiled.

The second principle advocates for privacy as the default.[99] PbD does this by advocating that manufacturers design their products with the maximum amount of privacy possible to begin

---

[94] CAVOUKIAN, *supra* note 7, at 1 ("Extending beyond FIPs, PbD represents a significant 'raising' of the bar in the area of privacy protection.").
[95] SETTLE, *supra note* 19, at 17.
[96] CAVOUKIAN, *supra* note 7, at 2 ("It anticipates and prevents privacy invasive events before they happen.").
[97] *Id.*("*PbD* begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently (for example, preventing (internal) data breaches from happening in the first place")).
[98] CAVOUKIAN, *supra* note 7, at 2 ("Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.").
[99] CAVOUKIAN, *supra* note 7, at 2.

with, only reducing it when absolutely necessary.[100] This principle incorporates the following FIPs: (1) purpose specification; (2) collection limitation; (3) data minimization; and (4) use, retention, and disclosure limitation.[101] If an organization does not absolutely require the data in question, it should not collect the data.[102]

The third principle is that privacy should be embedded into the design.[103] Similarly to SBD, products should be designed with the human user in mind. They should be shipped to the consumer in their most privacy-protective setting.[104] The manufacturer is the party best able to protect the customer's privacy. The burden should fall to the manufacturer, not the customer. Privacy protective settings should require a consumer to opt-out, not opt-in.

The fourth principle is that PBD should be approached in a positive-sum, not zero-sum, manner.[105] Manufacturers should look at information privacy holistically to see the net gain it provides.[106] Information privacy can and should be incorporated in a way that strengthens security and business processes.[107]

The fifth principle is that data should be protected throughout its entire lifecycle.[108] Organizations must ensure the confidentiality, integrity, and availability (CIA) of the data they possess.[109] Once the purpose for the data no longer exists, it should be destroyed in a manner that

---

[100] *Id*. ("Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.").
[101] *Id.* at 2-3.
[102] *Id.* at 3 ("Where the need or use of personal information is not clear, there shall be a presumption of privacy and the precautionary principle shall apply: the default settings shall be the most privacy protective.").
[103] *Id*.
[104] *Id.* ("The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error.").
[105] *Id.*
[106] *See* CAVOUKIAN, *supra* note 7, at 3.
[107] *Id.*
[108] *Id*. at 4.
[109] *Id*.("Applied security standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle.").

prevents anyone from subsequently accessing the data.[110] There is no justification for an organization losing track of the data it holds or failing to adequately protect it.[111]

The sixth principle is visibility and transparency.[112] This principle seeks to assure stakeholders the organization adheres to the claims it has made regarding the personal information it holds and processes.[113] This principle encompasses the FIPs of accountability, openness, and compliance. The sixth principle affords customers the opportunity to compare an organization's privacy practices with that of its competitors, allowing the customer to select an organization that best meets its needs.

Finally, the seventh principle is respect for user privacy, which requires that organizations bear the interests of their customers in mind when designing their products.[114] This principle incorporates the following FIPs: (1) consent; (2) accuracy; (3) access; and (4) compliance.[115] Products need to be tailored to the nature of their human users and provide clarity about the impact of collecting their customers' personal information.[116]

4. CASE STUDY

Lapsus$, a transnational group of threat actors conducting extortion-focused attacks, emerged in 2021.[117] They gained attention for having penetrated multiple well-known organizations.[118] Lapsus$' operations made use of penetration testing methods, social engineering, and initial access brokers (IABs).[119]

---

[110] *See id.*
[111] *Id.*("There should be no gaps in either protection or accountability.").
[112] *Id.*
[113] *Id.*
[114]*Id.*.
[115] *Id.* at 5.
[116] CAVOUKIAN, *supra* note 7, at 5.
[117] CYBER SAFETY REV. BD., *REVIEW OF THE ATTACKS ASSOCIATED WITH LAPSUS$ AND RELATED THREAT GROUPS REPORT* 1 (2023) https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf.
[118] *Id.*
[119] *Id.* at 3-4.

4.1. Gaining Initial Access

Initially, Lapsus$ would study their targets, collecting information on the intricacies of the business and its employees.[120] They would search their target's network to identify vulnerabilities that would allow them to penetrate the system.[121] SBD is critical to reducing threat actors' success rates with regard to vulnerable products. However, while SBD should effectively reduce the risk associated with vulnerable products, threat actors would still be able to penetrate IABs.

Where the attackers could not find suitable vulnerabilities, they would use social engineering to gain access.[122] Attackers achieved this by collecting publicly available information on their targets, such as "employee profile pictures, department structures, business processes, workflows, and business relationships."[123] This information-allowed attackers to impersonate both employees and customers, which allowed them to use a variety of phishing techniques to trick employees or customers.[124] Threat actors convinced employees or customers to go to "spoofed or hacked websites" where the attackers stole their login credentials.[125] Where they were unable to steal employees' credentials through phishing, threat actors would attempt to hijack the multi-factor authentication (MFA) process.[126]

Mobile phones, an ever-present component of daily life, are also integral in the MFA, SMS, and two-factor authentication (2FA) processes. Telecommunications providers are targeted because they are integral to the MFA process.[127] Telecommunication providers facilitate the delivery of the passcodes used to authenticate an individual's identity.[128] Penetrating

---

[120] *See id.* at 3-4.
[121] *Id.* at 4.
[122] *Id.* at 6.
[123] *Id.*, at 6-7.
[124] CYBER SAFETY REV. BD., *supra* note 117, at 6.
[125] *Id.*.
[126] *Id.* at 7.
[127] *Id.*, at 5.
[128] *Id.*

telecommunications providers or manipulating telecommunications providers through social engineering allows threat actors to insert themselves into the MFA process and thereby approve their own access requests.[129]

Threat actors put mobile phone customers at risk when they can use social engineering to make changes to customers' phone plans.[130] Threat actors' ability to impersonate mobile phone customers and change their services directly impacts the risk to those organizations that employ the targeted customers. In particular, Lapsus$ and other similar threat actors used subscriber identity module (SIM) swapping to move a customer's phone number to their SIM.[131] SIM swapping allows an attacker to then receive SMS, calls, and MFA-requests intended for their victim.[132] After successfully SIM swapping a customer's phone number, threat actors were able to approve access and gain control of their accounts.[133] Lapsus$ was able to do this because of the personal information they acquired about their victims.[134]

Alternative, threat actors sometimes use the MFA process force individuals to approve their MFA requests.[135] To create MFA fatigue and convince their targets to approve their access requests, attackers bombarded individuals with MFA requests until they could no longer tolerate the requests and approved them.[136] Occasionally, attackers would also use data they had previously harvested to impersonate IT personnel and trick individuals into approving the requests, believing that they were speaking with a legitimate employee.[137]

---

[129] *Id.*
[130] *Id.* at 27.
[131] *Id.* at 7.
[132] *Id.*
[133] CYBER SAFETY REV. BD., *supra* note 111, at 7.
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*

Telecommunication service providers face difficulty in improving these processes because they need to maintain a quality customer service experience to remain in business.[138] These situations include instances where a customer is travelling internationally, loses their phone, and is unable to verify their identity.[139] In situations such as these, telecommunication services providers have limited means of identifying an individual, making it easier for threat actors to impersonate the individual.[140] To effectively deal with SIM swapping and the exploitation of telecommunication providers, they need to develop more effective methods identity verification.[141] Here, had threat actors not been able to collect the customers' information, they would not have been able to effectively impersonate and defeat the telecommunication provider's verification process.

In some instances, they also used Emergency Disclosure Requests (EDRs) to get information about individuals they could use to gain access.[142] Government entities use EDRs to request records or data from service providers in emergency situations and receive an immediate response.[143]

Where threat actors could not find any useable vulnerabilities, they were able to source login credentials from IABs.[144] IABs use the same methods as Lapsus$ and other attackers to collect the necessary personal information to gain access.[145] Once they have used the personal information they collected to gain access, IABs "then sell it in online forums."[146]

---

[138] *Id.*at 27.
[139] *Id.*
[140] *Id.*
[141] *Id.* at 34-36.
[142] CYBER SAFETY REV. BD., *supra* note 111, at 4.
[143] *See id.* at 5.
[144] *Id.* at 4.
[145] *See id.* at 6.
[146] *See id.*

Instead of attacking their target directly, threat actors can gain access through a supply chain attack. Lapsus$ and other similar threat actors exploited the privileges their targets had provided to their third-party service providers.[147] Business process outsourcing companies (BPOs) are targeted because of the access they are granted in order to manage their customers' operations and because they provide access to multiple organizations.[148]

When contracting with a BPO, companies should consider what data the BPO will actually need to perform the contracted function. If that data is part of a larger set, the necessary data should be segregated. Additionally, BPOs should be granted the least degree of privilege possible. Failure to limit a BPO's privileges will increase the attack vectors a threat actor may use once inside the system.

Similarly, third-party service providers, such as software as a service (SaaS) providers, allow threat actors to gain access through the enterprise software their targets use.[149] Attackers were able to exploit vulnerabilities in Microsoft's Active Directory (AD), Exchanger Servers, Windows User Profile Service, and other such products that contained privileged access and information.[150]

4.2. Post Initial Access

After initially accessing their targets, attackers are able to then branch out and "compromise systems, software, identities, or network access."[151] Subsequently, they would take steps to normalize their presence in their target's environment.[152]

---

[147] *Id.* at 5.
[148] *Id.*
[149] *See* CYBER SAFETY REV. BD., *supra* note 111, at 5-6.
[150] *Id.* at 10-11.
[151] *Id.* at 6.
[152] *Id.* at 11.

Threat actors use documented internal procedures, information shared on collaboration platforms, and internal help desk ticketing systems, hosted by organizations, to enable their activities.[153] To elevate their privileges, attackers generally made use of unsecure passwords and keys, legitimate and illegitimate tools, and unpatched vulnerabilities.[154] Many of the organizations studied failed to secure their passwords and keys by storing them (1) in spreadsheets; (2) on Slack; (3) on collaborative platforms such as GitHub; (4) on internal enterprise knowledge sharing platforms; (5) embedded in a PowerShell script; and (6) on their browser password caches and keychains.[155] Had the passwords and keys been encrypted, or not even stored digitally on the network, attackers' progress would have been severely inhibited. Products such as YubiKey, hardware based multifactor authentication devices, should go a long way toward solving this problem. It would remove the passwords and keys from the system, and they would be held on the employee or customer's person.

Where threat actors used software tools, they used "a mix of system utilities, diagnostic extension, administrative databases, and [other] malicious tools."[156] Such tools were used by attackers for credential dumping, internal social engineering, virtual machine (VM) backups and log collection, and temporary credential creation.[157]

After gaining access, attackers would take efforts to conceal their presence on the network. They accomplished this by adding new accounts, establishing remote access, and circumventing security.[158] To circumvent the target's security, threat actors modified firewalls, exploited bring your own device (BYOD) policies, and installed malware on the system.[159] Modifying an

---

[153] *Id.* at 9.
[154] *Id.* at 9-10.
[155] *Id.* at 9.
[156] *Id.* at 9.
[157] *Id.* at 10.
[158] *Id.* at 11.
[159] *Id.* at 12.

organizations' firewalls allowed attackers to enable Remote Desktop Protocol (RDP) connections. RDP allowed them to control the system to which they had gained access from a remoted location.[160] When remotely accessing the target's system they used onion routing and virtual private networks (VPN) to conceal their identity and location.[161]

Where organizations had BYOD policies in place, attackers "used 'Bring Your Own Vulnerable Driver' (BYOVD) attacks to deploy malicious kernel drivers signed by stolen code-signing certificates (obtained from another targeted entity) to bypass security detection and disable security controls."[162] More significantly, however, they installed "BlackLotus," a "Unified Extensible Firmware Interface (UEFI) bootkit."[163] The threat actors installed BlackLotus because of the difficulty of detecting it and the degree of control it afforded.[164] Malware installed via a bootkit allows the code to get "up and running prior to the computer operating system on boot up."[165]

Information privacy appears at first glance to be an unnecessary inconvenience. However, when attackers are able to use that personal data to wind up successfully installing programs like BlackLotus, information privacy principles that were initially dismissed as a nuisance rapidly grow in importance. Poor information privacy practices have an outsized impact on cybersecurity.

4.3. Impact

While attackers were sometimes haphazard in exfiltrating data, scooping up whatever happened to be available, which was sometimes of little value, they were also able to target much

---

[160] *Id.*
[161] *See id.* at 4.
[162] *Id.* at 12.
[163] *Id.*
[164] Kurt Baker, *Bootkits*, CROWDSTRIKE (Jan. 5, 2003) https://www.crowdstrike.com/cybersecurity-101/malware/bootkit/.
[165] *Id.*

more valuable data. Through their attacks, the studied threat actors acquired intellectual property as well as user data.[166]

The intellectual property data attackers took included source code from a variety of technology companies, internal business communications, account information, medical information, and other personal information.[167] With this data, the threat actors were able to extorts organizations and individuals and disrupt services.[168] They were also able to use data to certify files containing malware with signatures to be used in further attacks. The accessibility and retention of this data within their victims' systems created the circumstances for the attackers to have the success that they did. Once threat actors got inside organizations, they were able to use their knowledge of an organization to further impersonate a variety of personnel with the organization, allowing them to manipulate otherwise into using their privileges to advance the threat actors' agendas.[169] The CSRB ultimately concluded organizations could not rely on technical cybersecurity solutions and that mastering basic cybersecurity practices were the only solutions that would help.[170]

4.4. Victim Response

In the wake of being targeted, organizations responded by increasing their security posture.[171] Wisely, one of the companies studied by the Cyber Safety Review Board (CSRB) prohibited BYOD in high-risk areas and instituted the principle of least privilege.[172] Organizations also began rotating their keys more often, effectively reset access. [173] Where they did not have

---

[166] CYBER SAFETY REV. BD., *supra* note 111, at 12.
[167] *Id.* 13-14.
[168] *Id.* at 12.
[169] *Id.* , at 27-28.
[170] *Id.* , at 28.
[171] *Id.* at 17.
[172] *Id.*
[173] *Id.*

BYOD policies in place, companies were able to require that traffic only come from their devices in order to access their internal network.[174]

MFA weaknesses received a great deal of attention for their role in enabling penetration. One organization stopped using SMS based OTPs and created a feature that allowed employees to flag authentication requests they thought may have been produced by threat actors.[175] Others began requiring their employees to re-authenticate more often.[176] One organization only allowed MFA that required employees to use a passcode on their screen to validate or leverage hardware-based authentication.[177]

Other general changes to MFA practices adopted by organizations were: (1) the use of phishing-resistant hardware tokens; (2) eliminating MFA push alerts; (3) verifying employee through video when resetting MFA; and (4) using Fast IDentity Online (FIDO).[178] These changes mitigate the inherent social engineering cybersecurity challenges presented when humans are involved in the system. Unfortunately, with the rise of generative artificial intelligence (AI), it will be possible for threat actors to fool video employee identification processes by generating videos of the employee whose identity the threat actor is using. Similarly, while hardware based authentication tools will mitigate the risk of penetration through phishing and social engineering, it is possible that they will put the safety of employees at increased risk. If a threat actor is not able to easily access an organization themselves, they may have to coerce an employee to give them access.

4.5. CSRB Findings And Recommendations

---

[174] *Id.* at 17-18.
[175] *Id.* at 17.
[176] *Id.*
[177] *Id.*
[178] *Id.* at 18.

The CSRB determined threat actors primarily exploited authentication and employee verification processes, and access weaknesses to penetrate their targets' systems.[179] Based on its observations, the CSRB recommended the cybersecurity environment be improved by strengthening identity and access management (IAM), mitigating inherent vulnerabilities in the telecommunications systems, and increase the resiliency third party service providers.[180] In accordance with the SbD framework, the CSRB asserted manufacturers should bear the burden of making the cybersecurity environment more secure.[181] Organizations will need to implement specific measures to mitigate the success of social of social engineering on humans; an opinion shared broadly across industry.[182] Software providers, hardware providers, and enterprises need to adopt solutions that recognize and account for this factor.

The majority of attacks involve social engineering at every step. Social engineering is used throughout an attack to gain initial access, information about the targeted, conduct SIM swaps, and defeat zero trust architecture (ZTA).[183] Technical cybersecurity solutions will not protect targeted organizations against social engineering.[184] Organizations' management of password databases and credentials allowed threat actors to acquire this data with ease.[185]

To minimize these threat vectors, organizations need to implement, by default, security measures that eliminate these opportunities for threat actors. Organizations should require authentication with hardware-based MFA each time an employee does something that requires privileged access to reduce the effectiveness of social engineering.[186]

---

[179] *Id.*at 12.
[180] *Id.*at 32.
[181] *Id.*
[182] *Id.*at 26.
[183] *Id.*
[184] *Id.*
[185] *Id.*at 32.
[186] *Id.*at 34.

5. WHY INFORMATION PRIVACY SHOULD BE INTEGRATED INTO CYBERSECURITY

Cybersecurity is a nationwide issue. It is not just about one company's program. Currently, they are viewed as distinct fields. They should be considered from a more holistic point of view. To develop and maintain a state of strong, nationwide cybersecurity, information privacy policies, practices, and frameworks should be incorporated as fundamental to cybersecurity programs. In this context, information privacy should be viewed as a framework for data protection.

Hacking today is generally achieved through the use of information, either to step through an opening or to gain improper access, not by overpowering someone else's ones and zeroes with your ones and zeroes. Ultimately, if the data on organizations and individuals that threat actors use to execute their attacks did not exist, they would likely be much less successful. While that is clearly impossible, it is not impossible to reduce the data that does exist and make it more difficult to aggregate. Organizations should focus on the PbD principles of proactive, not reactive, and privacy as the default, along with the FIPPs' principle of authority.

Lapsus$, as described earlier, used phishing and stolen credentials to penetrate organizations. Where Lapsus$ themselves did not phish organizations, the IABs from which they purchased stolen credentials had. Critical to the success of Lapsus$, similar threat actors, and the IABs was their ability to social engineer both employees and consumers. They were primarily able to do this because of the information they were able to collect about the individuals and the organizations.

Once inside an organization, they were able to move laterally through the network, from system to system. When necessary, they could sometimes escalate their privileges, allowing them access to a broader range of internal systems and data. Often, accessing one organization would allow them to move externally to another organization. This was used both to move from a service

provider to their customer and vice-versa. Their access, information about the business' internal operations, and the organization's failure to protect its data internally allowed them to succeed.

Ultimately, the FIPs, PbD, and other privacy frameworks are about protecting data, though their specific is to maintain the privacy of a data subject's information. In spite of that, they can be applied to data protection at large. Cybersecurity professionals need to incorporate information privacy into their tool bag to adequately address the threat of social engineering and to avoid providing threat actors with the tools they need to be successful once inside the network.[187] Both cybersecurity and privacy professionals ensure the entities for which they work protect the data they possess and use in a manner that is consistent with the current standard.[188] Cybersecurity professionals need to incorporate these privacy frameworks to meet the standard of reasonable cybersecurity.[189]

CONCLUSION

The amount of cyberattacks conducted annually is soaring. SbD will not suffice on its own to address this risk. While SbD will lead to secure products, humans still play a role in the security process, creating a perennial vulnerability. Threat actors exploit this vulnerability through social engineering in a considerable number of cyberattacks. The proliferation and bulk storage of personal information have enabled threat actors to conduct these attacks more efficiently and increased the potential harm as a consequence of successful attacks.

The magnitude of personal information stored and in circulation provides threat actors with the information they need to impersonate authorized individuals and gain access. It also increases

---

[187] COBUN ZWEIFEL-KEEGAN & ANOKHY DESAI, BUILDING THE NEXT GENERATION OF SECURITY AND PRIVACY PROFESSIONALS 12 (arguing that the best technical cybersecurity measures will leave gaps that only information privacy frameworks would address).

[188] *Id.*at 3 (International Association of Privacy Professionals 2022) (arguing cybersecurity and privacy professionals share overlapping roles).

[189] *Id.* , at 12 ("To meet industry standards, data security professionals must incorporate privacy best practices into their knowledge base.").

the financial risk to organizations where the cybersecurity incident is material or where a sufficient amount of unsecured data is exfiltrated. The FIPPs and PbD should be implemented in addition to SbD to reduce the potential harm of collecting and processing personal information. Combatting the impact of social engineering requires a comprehensive approach, addressing the different vectors that facilitate its success.