NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

THINKING BEYOND PII:

Policy Solutions to Address the Real Causes of Cyberattacks

By James W. McJunkin
Vice President & Chief Security Officer
Corporate Security
Discover Financial Services

Thinking Beyond PII: Policy Solutions to Address the Real Causes of Cyberattacks

In the United States, personally identifiable information (PII) is an excessive focus of most cybersecurity law, policy, and best practices from both the private sector and federal government. It's a tangible concept in the mind of the public and something very specific to give lawmakers a focus when discussing cybersecurity. Most state data breach notification laws, industry-specific regulations, and national policies use the successful or failed protection of PII as a yardstick – and sometimes using that measure to punish those who fail.

However, as the nature of cyberattacks grows more sophisticated, should PII remain our primary focus? In and of itself, PII is practically worthless. PII data sets are commonly sold on the dark web for prices as low as $10. So why has PII become such a high priority target for hackers? Simply because PII allows a criminal to effectively pose as a legitimate customer and thereafter effectively and consistently defeat authorization controls at most financial institutions. In this manner, criminals effectively (and anonymously) monetize PII.

Meanwhile, companies lose billions of dollars to fraud resulting from data breaches, and to cyberattacks stemming from root causes and consequences far beyond whether or not a company protected its customers' PII.

By focusing too much of our legislation, regulations, and national policies on PII, we limit our effectiveness at preventing modern cyberattacks and even protecting our country's national security. We must investigate **how** PII is used as part of wider cybercriminal operations, understand how organizations must protect their most sacrosanct components – the crown jewels of their operations – and then articulate clearer, better laws and policies that elevate cybersecurity standards in the United States. The purpose of this whitepaper is to create discussion around each of these three areas.

The Modern Attack Chain

A widely adapted although debated concept in cybersecurity is the kill chain, or attack chain, somewhat standardized in 2011 by a major aerospace company. The company's seven steps present a traditional view of the attack chain:

- Reconnaissance
- Weaponization
- Delivery
- Exploit
- Installation
- Command and Control
- Actions

Alternate models also describe linear, perimeter-focused attacks where the goal is for criminals to hack their way past a technological barrier. Some focus on post-compromise behavior.

However, when applied to modern cyberattacks, some issues emerge if we stick too close to these models. By overly focusing on the perimeter, linear attacks, and clearly unauthorized breaches, we miss the complexity of modern cybercriminal activity.

For example, a cybercriminal attacking a bank may use an attack chain that looks more like this:

- Various criminals hack multiple companies for PII.
- Criminals buy and sell PII on the dark web.
- A criminal poses as a customer to take over an account at a bank.
- More information is mined from an account takeover.
- Hacking reinvestments occur.

Notice the decentralization of these efforts. A bank – pouring all its efforts into the old attack chain model— is caught off guard. PII is not the main problem when it is already stolen from less secure companies having nothing to do with financial services and then bought cheaply on the dark web. If criminals use stolen credentials, they're inside the bank. Focusing primarily on protecting PII doesn't account for these criminal interlopers.

Of course, cyberattackers still attack the perimeter and commit traditional linear attacks. But modern cyberattacks are often multichannel, complex, and rely on less technical tactics such as social engineering.

In other words, PII is no longer the primary issue, although criminals use PII as part of their attacks. According to *Bloomberg*, "Underground markets also sell full identities of individuals just like you for as little as $10 apiece. They're called fullz, 'dossiers that provide enough financial, geographic and biographical information on a victim to facilitate identity theft or other impersonation-based fraud,' [an annual report on cybercrime by Secureworks, a unit of Dell Inc.] explains. Fullz can help a criminal get past those irritating 'secret questions' that sites ask to verify your identity."

Why do we fixate so heavily on protecting PII when it is bought and sold for the price of a sandwich? It's a tangible concept, especially for non-technical people. PII makes more sense to the public than multichannel fraud and complex attack chains. We value our tangible personal information stored by organizations, and we expect organizations to protect it.

But when our personal information does not just reside within a single company, then it is not the problem of a single company. Think about how many organizations currently have someone's social security number on file. Dozens? Hundreds? Now, what's the chance that the organization experienced a breach? It's high.

If PII alone is all but worthless on the black market, then what do companies need to focus on instead? Before we talk policy, we must understand a company's critical crown jewels of data and essential components.

What Are Your Organization's Crown Jewel Components?

Technologists often like cut and dried tasks to measure. If you assume PII is what criminals want, then you build technological barriers around PII and prevent a breach. It's no different than assuming an army wants the treasure in your castle—so you pour all your efforts into fortifying and defending the castle to protect the treasure.

But what if, while defending the castle's treasure, an enemy enters through an unguarded door, takes over your drawbridge, and accurately imitates the king? Similarly, if PII by itself is no longer a crown jewel because of its prevalence on the dark web, then what should you protect?

In today's information security climate, a company's critical dependencies may represent examples like the following:

Revenue

Criminals don't want your PII. They want your money. In industries such as financial services and retail, that means they focus on specific strategies and tactics that siphon off revenue such as account takeovers, reshipping, or Card Not Present fraud. PII is simply a means to an end—and an end that was originally designed by financial institutions traditionally focused on detecting first party fraud (from the customer). In fact, third party criminals (non-customers) using stolen PII to achieve the transparent appearance of a customer are responsible for the majority of fraud and credit loss. PII is just part of a complex set of data that cybercriminals use to access your products and services—leaving you on the hook for the charge.

Reputation

Your reputation is a valuable jewel—for many reasons. Criminals often breach organizations not only to steal money but also to make a point, embarrass a company, or enact revenge. Recent cyberattacks on large, well-known companies have not only affected the reputations of those companies but also caused the public to lose confidence in entire industries. Hits to reputation also affect shareholder value and sometimes put companies out of business.

Employee data

Protecting customers' PII is important, but employee information is another critical data set. Two of the biggest data breaches in history—one involving a data security company and the other involving the US government's Office of Personnel Management (OPM)—both exclusively focused on the theft of employee data. The data security company's breach affected 40 million employees and the OPM breach affected 22 million employees, both current and former. With employee data, cybercriminals can potentially pose as employees and access classified, sensitive, and unauthorized information.

Critical infrastructure and services

In some cases, a company's crown jewels are the critical services it provides society. Obvious examples include electricity, oil, gas, water, sewage treatment, hospitals, telecommunications, and data centers. Also included are services that keep the economy running. For example, one digital payments company now processes about 20 percent of the world's credit card transactions. A criminal – especially from a nation state or organized crime ring – going after any of these organizations is not going after PII. They are seeking to take down that company's operations to cause substantial public harm and economic disruption.

Criminals are going after much bigger targets than PII – and targets that cause extensive harm to not only single organizations but also to entire industries and societies. Therefore, a primary focus on PII is no longer tenable in such an environment.

Given these critical components as targets, organizations would be wise to consider expanding their cybersecurity strategies with laws, regulations, and policies to match the following strategy:

Transition from a one channel to a multichannel cybersecurity defense mindset.

If we acknowledge the multiple channels that hackers use to infiltrate a company, we see that defending a traditional perimeter is not a sufficient strategy. Criminals use a combination of:

- **Physical security breaches**: While onsite, a criminal can talk their way past a security guard, pretend to be someone they're not, and extract information. Methods include taking photos of written down passwords, using flash drives to quickly steal information off a laptop, or hacking into a network from an unused computer.
- **Phone breaches**: Criminals can use social engineering tactics to trick call center representatives, helpdesk staff, and employees into giving up sensitive information over the phone.
- **Online security breaches**: Criminals can use information gleaned from physical and phone breaches to access information online.

Focus on holistic versus solely technical security.

Too much thinking about cybersecurity in Washington, D.C. involves technical tactics. In other words, is an IT team protecting bits and bytes? However, this kind of thinking about information security allows non-technical decision makers to avoid responsibility, removes them from the process, and abdicates any cybersecurity responsibility they own.

Cybersecurity is far more than its technical elements. Overall business strategy, policies, procedures, and governance forms the foundation upon which an organization thinks about security. For example, if only the IT team is worried about cybersecurity, then how are non-technical employees trained to spot physical security breaches? What about the security procedures in a call center? What about enacting a crisis plan after a breach that involves executive leadership, the board, and public relations?

Focus more on combating disguised criminals.

Of course, many intrusion prevention solutions exist to prevent criminals from unauthorized access to data. But what about seemingly legitimate criminals who enter with stolen information – either from their own efforts or the dark web? We need to devise strategy and policies that do a better job of detecting and mitigating “malicious behavior” common to most customer account systems and account for criminals who smooth talk their way into fraud. Every cybercriminal will not appear like a traditional hacker. Organizations and policymakers need to discuss ways we can better authenticate people, look for red flags, and spot suspicious behavior that focuses more on how criminals actually perpetuate cybercrime.

Widen the definition of information to protect.

Beyond PII, other information becomes extremely valuable to an organization – and to a criminal – that also relates to people’s privacy and security. For example, better protecting authentication procedures, intellectual property, internal employee data, and operational/business continuity data all could lessen the risk of a data breach, privacy violation, or, in a worst-case scenario, a public disaster.

Strengthen public-private sector information sharing and partnerships to combat and counter sophisticated threat actors such as nation states and organized crime rings.

At one point, industries going it alone in cyberspace made sense. Companies within each industry protected themselves and perhaps participated in ISACs to share information about threats. For a long time, the federal government was largely not up to the task of a robust partnership with the private sector. Today, everything has changed. The Department of Homeland Security (DHS) and others are realizing past mistakes, doing a better job of correcting them, and reestablishing connections with the private sector.

DHS is now offering more relevant services that can benefit companies. Militarily, US CYBERCOM is now a combatant command and seeks more partnerships with the private sector to fend off nation state and organized crime attacks. And many federal agencies seem to be coordinating efforts toward a solution that requires a unified strategy between the public and private sector around cyberthreat intelligence information sharing to protect our national security.

We need to understand that our cyber adversaries are well-trained and well-financed, and we must respond with a more effective and coordinated approach that uses intelligence to identify new and evolving Tactics, Techniques and Procedures (TTPs) and tradecraft, not just Indicators of Compromise (IOCs). Then, we must share that information outside of the government with private sector partners. In today's environment, we must play chess, not checkers, with the criminal groups that seek to profit illegally using anonymous and largely untraceable methods of attack.

This kind of strategy is a far cry from simply forcing individual companies to protect customer PII. Instead, it requires dialogue, intelligence sharing, and strategizing about the best ways to coordinate between the public and private sector when a nation state, sophisticated organized crime ring, or other significant threat actors attack US companies. Instead of blaming a single company for failing to protect personal information, the mission has evolved toward working together to make cybersecurity better for all organizations.

From Vision to Legislative Reality

Perhaps this strategy sounds too good to be true. While GDPR will have a ripple effect on US data privacy through many global companies and organizations changing data privacy policies for all, not just EU, customers, many organizations will still build policies and carry out cybersecurity strategy that only reacts to a confusing patchwork of US laws.

While NIST publishes guidelines and recommendations about PII, they are not law. Current legal definitions of PII are specific, contradictory, and varying. As stated before, there are other kinds of information that may not be covered by PII laws that can be weaponized in an attack or combined with PII to attack companies – making PII-focused laws ineffective at making companies truly secure. For example, quasi-identifiers or pseudo-identifiers (such as a birthdate or a postal code) may be used to commit a data breach, but current US law may not see this information as valuable enough to protect.

Complicating the picture, there are 50 data breach notification laws from each state plus the Virgin Islands, Guam, Puerto Rico, and the District of Columbia. Then add industry-specific laws such as HIPAA, HITECH, Gramm-Leach-Bliley, the CFPB, and many others. Each law may define PII somewhat differently. That means a company operating in one state or industry may be legally required to protect specific data that doesn't need protection in another state or industry.

The absence of a GDPR-like national law around PII in the US gives us the opportunity to think beyond simply the protection of a limited amount of data when considering legislation and policy that makes sense for consumers, businesses, and national security. Any proposed legislation – instead of just fixating on yet another definition of PII – can instead consider:

- **National data breach notification legislation**: Having one definition of notification requirements for organizations will help create a national standard, reduce contradictions, and get everyone on the same page about what constitutes a data breach and how to report it.
- **Stronger public-private information sharing**: Instead of leaving US companies on their own to fend off a vast variety of threat actors, the partnership between the public and private sector must grow stronger. Steps are already occurring to strengthen this partnership, led by organizations such as the DHS, US Cyber Command, and others. But more dialogue and interaction needs to happen.
- **More help and less punishment from the federal government.** It makes great theater to publicly shame companies when a major data breach occurs. Lawmakers can score points with an angry public by punishing those companies through legislation. But is that a good long-term strategy? We need more assistance from the federal government to help businesses detect, identify, prevent, and fend off sophisticated attacks from nation states and organized crime rings. For example, DHS programs such as Automated Indicator Sharing (AIS), the Cyber Information Sharing and Collaboration Program (CISCP), and Enhanced Cybersecurity Services (ECS) help companies that may struggle to fend off cyberattacks.
- **Better legislative and regulatory requirements.** Requirements are needed for information security policies that go beyond defining and protecting PII. For example, the FTC has the authority to punish companies for lax data security while not providing guidelines or best practices. Federal and state laws conflict and seem to focus more on reporting requirements after a data breach instead of requiring preventive security measures that would actually help increase cybersecurity standards. Laws, regulations, and policies can better define authentication standards, cyber hygiene requirements, more secure business processes, and a focus on protecting valuable non-PII information.
- **Better incentives and penalties tied to business metrics**. Boards, executive leadership, and legal teams are less prone to care about cybersecurity if it is all the CISO’s fault. But if cybersecurity laws, regulations, and policies were tied to revenue and brand reputation, then organizations will be more incentivized to change. For example, what percentage of budget is an organization spending on cybersecurity? Is it appropriate? What does governance look like? Is cybersecurity at the table and talked about at every board meeting? Are there real consequences for executive leadership and shareholders in the wake of a data breach or cybersecurity attack?

Many stakeholders are already headed in a new direction. CISOs, the DHS, US Cyber Command, many lawmakers, and groups like the National Technology Security Coalition have begun the dialogue and planning needed to evolve the way we think about cyber threats and what we protect within our organizations.

I envision a day in the near future when the private and public sector are working hand in hand to combat these threats. Sharing information, understanding the enemy, and taking measures to steadily improve our cybersecurity posture will happen – supported by pragmatic, robust, and reasonable legislation that matches the reality we face.

As a member of the NTSC Board of Directors, I am excited that this organization of CISOs – with a non-partisan, industry-agnostic approach – will raise its voice in Washington, D.C. to work with Congress to draft, adapt, and evolve our national policy around how we protect companies – thinking beyond PII to how the efforts of each and every private sector organization all work collectively to help increase national security instead of punishing those single companies that fail.

Mr. James W. McJunkin is a Vice President/CSO at Discover Financial Services, previously serving as the CISO. Prior to Discover, Mr. McJunkin spent nearly 30 years in state and federal government as a law enforcement professional, culminating with his service in significant senior executive leadership positions within the Federal Bureau of Investigation (FBI). He is a graduate of Penn State University and received his CISO certification from Carnegie Mellon University.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION