February 2018

Security Awareness News

the security awareness newsletter for security aware people

Compliance & Me

Getting Comfy with Compliance

Regulations Near & Far

Following Policy and Reporting Incidents

Getting to Know NIST

© The Security Awareness Company, LLC

Getting Comfy with Compliance

Think about the last time you opened a bank account, or when you first visited a doctor, or made a purchase online. What information did you need to provide? ***Full name. Phone number. Date of birth. National identification number. Maiden name.*** In some cases, maybe even job and salary information or previous health issues. ***Physical address. Email address…*** and we're just getting started.

Personally identifiable information, or PII, is as valuable as currency. It's our ticket to accessing things like healthcare and credit cards. We have to surrender a ton of PII in order to acquire basic services, such as electricity and internet access. The question is, **how is that information being protected?** Who is allowed to access it? And what happens when it's compromised?

Enter compliance regulations.

From the healthcare and payment card industries to international cross-border transactions, our PII is collected, stored, and transferred by hundreds of entities worldwide. Without compliance regulations, there would be no standardization for securing that data. There would be no formal process for the who, what, when, and where of our PII. There would be no rights for us as individuals should someone improperly access or transfer our data.

Regulations are a vital part of our connected society. They are the only way we can ensure the **confidentiality, integrity, and availability** of sensitive data. What does this mean for you personally? The next time you fill out a form, either in person or online, make note of how much info you must provide. And be sure that the party receiving the info is legitimate.

Here at work, it's your responsibility to know what compliance regulations our organization must follow. ***You should also know our internal policies regarding sensitive data. If you're not sure, please ask ASAP!***

The CIA Triad

The concepts of confidentiality, integrity, and availability—the three components of security that set the standard for how we handle sensitive information—have been around for centuries. Information always has been and always will be a sought-after commodity. The CIA Triad operates as the fundamental starting point for protecting data.

Confidentiality

Confidentiality equals privacy. Keeping data safe and secure is an integral part of information security.

Integrity

What's worse, data being stolen, or data being changed by an unauthorized party? It's sort of a trick question, but many security experts believe integrity is the most important part of data.

Availability

Data without availability has no value. If you accidentally delete something or if a backup fails, the data is gone forever. If our networks fail, the data is inaccessible—no different than being deleted. Availability is crucial to our operations.

© The Security Awareness Company, LLC

Regulations

Near & Far

Governments and regulatory industries around the world have recognized the need to prioritize the security of personal information. Each passing year, new laws and compliance standards are put into motion. Unfortunately, not every country has robust data protection laws like those of the United States, Europe, Australia, and China.

We can only hope that, as privacy becomes a matter of international and personal security, more countries will ramp up efforts to protect their citizens. To see a world map of existing laws, and to compare countries across the globe, check out this website:

https://www.dlapiperdataprotection.com/index.html?t=world-map&c=CN

GDPR

In April of 2016, the European Union (EU) adopted a new law called the **General Data Protection Regulation** (GDPR). Many consider this the new gold standard of cross-border data regulation. The GDPR applies to any organization that accesses personal data of an EU resident, regardless of where the organization is located worldwide. The mission behind the GDPR is to update technologically-irrelevant standards from 1995, to make regulation easier for organizations, and to maximize the protection of EU residents. Read more:

https://www.thesecurityawarenesscompany.com/2017/12/07/what-is-the-gdpr/

Privacy Shields

Even though the US has robust data protection laws, the EU considers some of those laws inadequate. To address this problem, government entities worked together to develop two frameworks: the **EU-US Privacy Shield**, and the **Swiss-US Privacy Shield**. Similar to the GDPR, the Shield program was created to assist US-based organizations in transatlantic commerce where accessing sensitive data is necessary. However, unlike the GDPR, neither framework is a regulation. Both require self-certification, which then makes the framework enforceable under US law.

How does Privacy Shield relate to the GDPR?

The GDPR requires that data may only be transferred to countries deemed to have adequate data protection laws, which the US does not. The Privacy Shield satisfies that requirement and allows organizations to access data across borders. Read more: **https://www.privacyshield.gov/Program-Overview**

Cybersecurity Law China

Adopted by the National People's Congress in November 2016, and officially activated in June 2017, China's Cybersecurity Law presents a significant upgrade of data privacy in the world's second largest economy. China already had various laws and regulations in place. The Cybersecurity Law further **defines how personal data may be collected, stored, and transferred,** and it expands the rights of individuals. Read more:

https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

Japan's APPI

Japan's Act on the Protection of Personal Information, or APPI, is one of the longest-standing cybersecurity laws in Asia, dating back to 2003. In 2016, Japan appointed the Personal Information Protection Commission to supervise and enforce amendments to APPI, the goal of which was to modernize Japan's data protection efforts. One of the biggest changes to the law was the introduction of restrictions for cross-border data transfer. **Business operators may not transfer personal data to foreign countries unless the individual has provided consent** in advance, and the country receiving the data has adequate protections in place. Read more:

https://www.lexology.com/library/detail.aspx?g=efa0a2b0-b73e-456c-b4fa-26a268e9e751

Why All This Matters

A common thread among the laws and regulations we've covered here is **cross-border data protection**. The harmonization of data laws across borders serves two vital purposes: it stimulates the global economy, and prioritizes the need for data laws worldwide. Cybercrime is a global threat that sees no borders and has no biases. We all play a role in preventing cybercrime. At work, that means following policy, reporting incidents, and thinking before clicking. At home, it means protecting personal devices with strong passwords, staying informed, and having conversations with friends and families about cybersecurity!

© The Security Awareness Company, LLC

Following Policy and Reporting Incidents

Policy (noun) -
"a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body"

You've probably heard "always follow policy" more times than you care to count. Indeed, we throw this phrase around a lot, and many organizations use it as a default slogan. And for good reason!

Without policies we invite chaos, which would undermine our efforts as workers and human firewalls, into our culture. We would have no way to ensure the protection of sensitive data, and no way to know if we maintain compliance of various regulations. Worse yet, without policy, the likelihood of a security breach significantly increases.

So, don't think of policy as arbitrary rules thrust onto employees. Instead, view policy as a fundamental part of your job function—strategic procedures that were carefully designed and implemented to ensure the success of our organization.

Want to know more about why certain policies are in place? Please ask!

Incident Response (noun) -
"an organized process of reacting to a potential security incident with the intentions of reducing negative impacts, and preventing future incidents"

We do everything we can to prevent security incidents. In fact, that's what following policy is all about: being *proactive* instead of *reactive*. But, despite our efforts, incidents will occur. How we respond to them is almost as important as how we prevent them.

As the name suggests, incident response is identifying and reacting to a situation that puts our organization at risk in some manner. Whether it's a threat in the Cyber Domain, Physical Domain, or People Domain, reporting the event and responding in a timely manner could be the difference between a major breach, or a minor setback. To read more about what an incident response plan is, check out this blog: http://secaware.co/2mytZRG

What Should You Do?

Analyze each of the incidents outlined below.
How would you handle them? What risks do they pose to our organization?
Do you know how and where to report them?

Incident Scenario #1:

You receive an email that appears to come from a co-worker, but the grammar is odd and there's a sense of urgency within the message. There's also a link to an unfamiliar source that the sender begs you to click on.

If it seems phishy, it probably is. This scenario looks like a spear phishing attack, which is a sophisticated form of social engineering that uses spoofed email addresses to trick people into sending money or clicking on malicious links/documents. We must report phishing emails immediately so our organization can alert other members!

Incident Scenario #2:

You find a USB drive in the parking lot far from the front door of our building. The drive is labeled with a sticker that says "financials", suggesting that it contains important, sensitive information.

Unexpected gifts from strangers should always tweak your security awareness as well as your inevitable curiosity. Social engineers often load USB drives and other plug-in media with malware and drop them in public areas, knowing that someone will pick them up and plug them in. Please, never give-in to such a temptation, whether it be a work or personal device. Report it!

Incident Scenario #3:

You notice a co-worker enter a secured area of our organization and hold the door open for someone that clearly doesn't have a badge or authorized credentials.

This is called piggybacking, the process of allowing someone to use your authorized access. Your co-worker, in this case, knowingly created a security event and you need to report them. This scenario is also related to tailgating, a situation in which someone uses your authorized access without you knowing (like sneaking in behind you). Don't let this happen to you! Stay alert, and look-out for those who don't belong.

© The Security Awareness Company, LLC

THINK ABOUT SECURITY DIFFERENTLY WITH THE NIST CYBERSECURITY FRAMEWORK

As our organization increases its resiliency to cybercrime, one of the things you may hear about is the **NIST Cybersecurity Framework (CSF)**. What is it and why does it matter?

Initially developed for critical infrastructure, the National Institute of Standards and Technology (NIST) established a framework to guide organizations in improving their abilities to prevent, detect, and respond to cyber attacks. This framework includes guidelines for policy, training, processes, and technical controls. Even though it's relatively new, many organizations across the United States will be using it in the future. (To learn more: https://www.nist.gov/cyberframework)

The core of NIST CFW has five components, providing a road map to stronger cyber-threat defenses. We believe our entire organization will benefit from learning about the process. It might even spark some new ideas, or lead you to think about common security problems (and solutions) in new ways!

IDENTIFY → PROTECT → DETECT → RESPOND → RECOVER

START OVER AND DO IT AGAIN!

IDENTIFY

"Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."

One of the most crucial steps to protecting any organization from cyber attacks is identifying vulnerabilities. In order to do that we need to know what assets we have and how those assets are valued by cybercriminals. This is known as risk assessment. Without it, we can't develop a risk management strategy. And an organization without a risk management strategy is one whose day-to-day operations have no defense against a continuously growing environment of cybercrime. By analyzing what we have and what we do, we can then identify vulnerabilities and focus our efforts from a top-down system per our business needs.

PROTECT

"Develop and implement the appropriate safeguards."

Protecting any organization starts with the people of that organization, which means your favorite thing ever: awareness and compliance training. It also means developing policies to mitigate our risk and punishing those who circumvent those policies. It means routinely auditing our users so we know who has access to what, and updating access controls accordingly. Safeguards also include investing in the appropriate technologies to monitor networks, and maintaining both hardware and software components so that updates are current and they are not left vulnerable to security holes.

DETECT

"Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

Detecting threats in a timely manner can mean the difference between suffering a massive breach and eliminating the threat before it has a chance to do real damage. To assist us in this area, many software and hardware companies offer services like real-time network monitoring, intrusion detection, phishing campaigns, etc. But this is also a human issue in that every single one of us needs to stay alert and be on the lookout for potential attacks at all times.

RESPOND

"Develop and implement the appropriate activities to take action regarding a detected cybersecurity event."

Our entire cybersecurity strategy is only as good as our incident response plan. Why? Because we are always in a "when, not if" environment. This is why we have the procedures in place so everyone can quickly assess a potential attack, and know immediately how and where to report said attack. Think of it as an emergency plan that establishes a set of protocols—a step-by-step policy—to mitigate further damage and increase the success of recovery.

RECOVER

"Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

Unfortunately, security events happen often. We know that. A proper recovery plan, however, at least mitigates the fallout, helping us pick up the pieces and restore systems back to full strength in a timely manner. It's also a chance to implement lessons learned from the incident, thereby strengthening our defenses against future attacks. Without a recovery plan, we would have to scramble to resolve issues, which costs time and money, and increases the scope of damage.

WANT TO LEARN MORE? *The NIST website is full of resources and tools to help us all better understand the framework and how it can strengthen our collective security efforts. Included are videos, webcasts, presentations, a detailed FAQ, and many articles. If you have questions, ask!*

© The Security Awareness Company, LLC