October 2018

SecurityAwarenessNews

the security awareness newsletter for security aware people

Time Is Not On Your Side

Types Of Incidents To Report

Incident Response
In All Three Domains

WHAT IS POLICY?

Time Is Not On Your Side

For almost three decades, we have harped on the single most important security awareness rule you should follow: **"See something? Say something." Or, "Report it now!" Or, "Report all potential security incidents IMMEDIATELY!"**

Why the urgency? Why is **IMMEDIATELY** so necessary? Why can't you wait until after lunch to report an incident? Why should you choose to be three minutes late for a meeting just so you can report a security incident? **Because resolution is all about time.**

Think about it this way: You notice something a little odd, or different, or unusual, and think it should be reported. It could be in any of the Cyber, Physical, or People domains. From your view, the security incident is new, but you don't know how long it might have gone unnoticed. You don't know if it has caused any harm or not… because you just noticed it.

Now think: How much damage can a security incident cause in one minute? How much damage can that same security incident cause if left unreported for one hour? Is that 60 times the potential damage? Or what about one day, or even a week, or longer? You simply don't know; all the more reason to report *any* suspected security event as quickly as possible.

Advanced Persistent Threats (APTs) often go unnoticed and unreported for more than a year.

The longer a security event goes unreported, the more potential there is for it to cause damage. **Advanced Persistent Threats (APTs) often go unnoticed and unreported for more than a year.**

How much information can a criminal or hostile nation-state steal in a year? How much money might be lost? How much damage can be done? The answer? WAAAY too much…

Better security is achieved by increasing the speed of security event *detection* and *reaction*. Detection is the moment you notice a potential security event. Reaction time is how fast you report the incident. The amount of time you take to detect and react (or report) is also called exposure time; the time during which you or your organization are potentially more susceptible to cybercrime.

If the first goal of information security is to reduce security events, then the second goal is to reduce the exposure time of those events. How do you that? By staying alert. By always following policy. And by never assuming an event doesn't matter or isn't "big enough" to report. **If you have any questions, please ask!**

tick-tock… tick-tock…

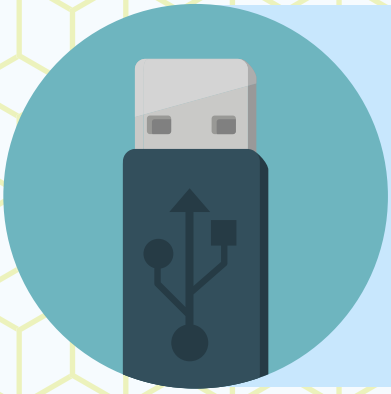
Types Of Incidents To Report

Phishing Emails

According to the 2018 Verizon Data Breach Investigations Report, one of the most troubling figures was not how many people fell for phishing attacks; rather, it was how many people failed to report them. Only 17% of phishing attacks were reported. This failure of communication destroys an organization's ability to both detect and respond. As human firewalls, our responsibility is to first identify when we're being attacked, and then to report that attack ASAP.

Unfamiliar Persons

It's normal to see an occasional service tech or delivery person in or around our organization. But the worst thing any of us can do is **assume** that someone has a right to be where they are. Social engineers have long used disguises to gain unauthorized access to freely roam around secure areas. That may sound like something that only happens in the movies, but art imitates reality. If you **ever** see any unfamiliar persons, verify that they have authorized access.



Random USB Drives

Curiosity is one of the easiest paths to hacking humans. That's why social engineers leave random USB drives in parking lots or hallways. They are confident that someone will find one of these "treasure chests" and feel the temptation to plug in the drive and view its contents. The problem? The contents could be malware that compromises an entire network. If you find a random USB drive or any other form of portable media, don't cave to temptation! Instead, report the incident and dispose of/turn in the item according to policy.

Vishing Attacks

Scammers don't stop at phishing emails. They'll happily call organization phone numbers and make false claims about needing sensitive information. This is known as vishing or voice phishing. This technique works on unsuspecting individuals because talking to a scammer in real life automatically creates a channel of trust, unlike phishing emails where you never hear a human voice.

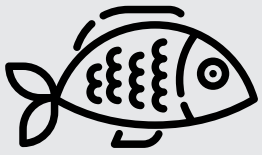
Incident Response In All Three Domains

The Cyber Domain

This domain goes well beyond just the internet. It also includes our computers, smart devices, printers, IoT, networks, and the software that makes it all work together. Sometimes it is easy to spot incidents in this domain, sometimes it isn't. That is why we must stay up-to-date and ever vigilant.

Bernard received a phishing email.

Bernard accomplished the first step to successfully thwarting an adversarial phishing campaign: he **recognized** that he was being phished. But his responsibility as a human firewall doesn't stop there. Just because Bernard was alert enough to spot the attack doesn't mean his co-workers would do the same. By reporting it, the organization can spread the word and warn others, effectively preparing everyone for subsequent attacks.



The Physical Domain

Did you know that a messy desk is a security risk? Do you log off of your computer every time you get up, even if for just a few minutes? Do you ever leave or see sensitive documents in the copy room? Are you familiar with dumpster diving? The physical domain has many tangible threats that are simple to isolate and simple to avoid.

Logan found a USB drive.

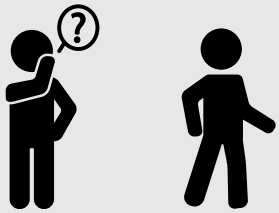
On his way from the parking lot to the front door, Logan spotted an unlabeled USB stick. Thankfully, he knew that criminals often intentionally place malicious USB drives around an area with hopes that someone will find them and plug them in. But if he didn't tell anyone else, how could he guarantee that it was a random event and not a targeted attack? What if there were actually **several** USB drives planted around the organization? Remember, time is not on our side. The sooner we can inform everyone within our organization of an incident, the better our chances of mitigating damage.

The People Domain

Not every threat involves the internet or malware and viruses. The people we interact with—our co-workers, suppliers, partners, even package delivery people—all represent potential security risks. Unauthorized access to secured areas is no different than hacking a database, because both scenarios threaten our overall security.

Elsie noticed an unfamiliar person in a secured area.

What would you do if you saw someone you didn't know or recognize walking around our organization? What if that person had a badge and claimed to be a service tech? Hopefully, you would do the same thing as Elsie. She asked the tech to wait in an approved area and she contacted management to confirm he was scheduled to be there. Once again, **never make assumptions**. If you're unsure of something, please ask!



What Is Policy?

Policy is a customized set of guidelines that an organization develops and implements to reduce security incidents. We ask that everyone within our organization follow our internal guidelines, and understand that they are not arbitrary. If you have questions about a policy, need clarification, or would simply like more information, please ask!

5 Reasons Why Policy Is So Important

1

It helps us manage our risk.

Policies exist to help establish which compliance regulations must be followed, how data is classified, who gets access to that data, and for how long. Without policies, organizations could not overcome the challenges of identifying the what, when, where, why, and who of information security.

2

A proactive approach prevents incidents.

Security incidents happen. They happen less often when policies are in place (and followed). For example, if we require that all work-issued mobile devices be encrypted, and someone accidentally loses or has a device stolen, we don't have quite as much to worry about because our policy protects us. If that policy is ignored of even bypassed, and a lost device ends up in the wrong hands, we could be looking at a data breach.

3

Policy assigns accountability.

This is not about placing blame when incidents occur. It's about having a system in place to retrace steps and determine what can be done to ensure that the incident won't occur twice. Policies essentially create a system of checks and balances, so we can quickly assess situations that involve human error.

4

It increases efficiency.

Imagine if every time we bring in a new hire, there were no specific policies or procedures in place and we had to start from scratch to onboard that person. It would consume a lot of time and resources. With new hire policies and procedures already designed and implemented, we can quickly place new employees into our workforce and bring them up to speed without much downtime. The same policy efficiency will come into play when offboarding employees.

5

Policies raise overall awareness.

From password creation to access controls, policies do more than simply build a set of rules for everyone to follow. They spread awareness of what it means to be strong human firewalls and how every individual in our organization is a valued member of our cyber defense. Remember also, that many of our guidelines can and should be utilized in your personal life, as well!

!

Don't Be The Insider Threat!

There are two specific types of insider threats: malicious and inadvertent. Even if you don't have malicious intentions, failure to follow policy puts you into the first category. Don't be that person! Always follow policy, no matter what, and help keep our organization resistant to security incidents.