SecurityAwarenessNews

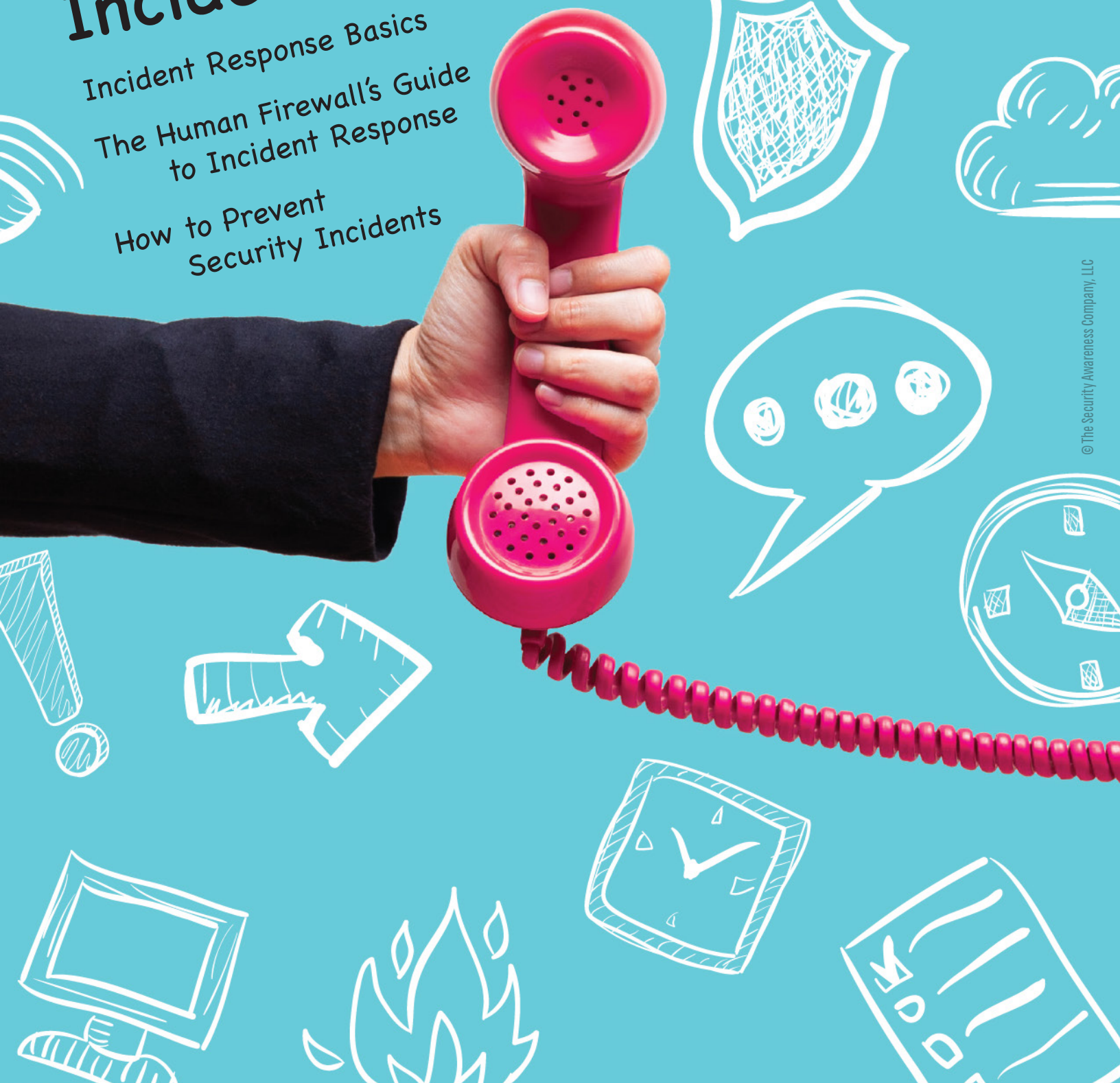
the security awareness newsletter for security aware people

Incident Response

Incident Response Basics

The Human Firewall's Guide to Incident Response

How to Prevent Security Incidents



Incident Response Basics

What is incident response?

Incident response refers to the processes an organization employs to help detect, respond to, and recover from security incidents. It's essentially an emergency plan with step-by-step guidelines, similar to how most buildings have predefined evacuation routes.

What are the steps of an incident response plan?

While every organization may have different structures and terminology, generic steps of most plans include:

- **Preparation -** compile a list of assets, and identify risks to those assets.
- **Detection -** discover and analyze the security incident.
- **Containment, Eradication, and Recovery -** contain the incident, remove the threat, and restore affected assets.
- **Post-incident analysis -** determine how the incident occurred, and take measures to reduce the probability of similar incidents in the future.

Why is incident response so important?

Failing to prepare is preparing to fail. Incident response plans set the stage for accurate and efficient recovery from security incidents. Without a plan, organizations would struggle to quickly identify threats and mitigate damages.

What's your role regarding incident response?

An organization's incident response plan won't work unless employees report incidents as soon as they notice them. Your role, therefore, is to stay alert and report incidents immediately. The longer something goes unreported, the more damage it could cause.

What's an example of reporting incidents?

Imagine you have a keycard that grants you access to a highly secured area of a building. One day, you come to work and find the door to that secured area left open. You could simply close the door and go about your day. But doing so prevents your organization from investigating the incident. Why was the door left open? Who left it open? Was it just a mistake? Did someone manage to break in? None of those questions get answered if you fail to report the incident.

In short, an incident response plan empowers our organization to develop policies that prioritize the security of our employees, clients, customers, and business associates. If you have any questions or need more information, please ask!

The Human Firewall's Guide to Incident Response

Preventing security incidents tops the human firewall's security to-do list. Just below "preventing incidents" on that list, we find "reporting incidents."

Stay alert.

Letting your guard down, even for a minute, could leave you vulnerable. Staying alert means treating all requests for sensitive information with a high degree of skepticism, locking your workstation when not in use, ensuring secured doors stay locked, and keeping an eye out for anyone who doesn't belong.

Don't assume something is too small to report.

So, you found a USB flash drive in the parking lot. No big deal, right? What if it contains malware and was intentionally planted by a social engineer? There are no incidents too small to report, and it's always better to be safe than sorry.

Know whom to call.

It's your responsibility to know how and where to report incidents. If you're unsure of whom you should report incidents to, please ask, so you're not left guessing should a situation arise.

Report it immediately.

Time is not on our side when it comes to security incidents. As such, reporting incidents promptly is one of the most crucial steps. The sooner you alert our response team to a potential threat, the quicker we can assess and remedy the situation.

Always follow policy.

While responding to incidents in a timely manner (immediately) is one of the top responsibilities of human firewalls, preventing incidents from ever happening in the first place is the optimal goal. You can do that by always following our organization's policies, which were specifically designed to reduce security incidents.

How to Prevent Security Incidents

The truth about incident response plans is that while they're absolutely necessary, we hope to never use them. You can help us by exercising these basic security awareness muscles daily:

Click with caution.

Phishing and smishing (phishing via text message) still hold the top spot on the list of "why data breaches happen." Even when an email appears to come from someone you know (such as your supervisor or co-worker), think before you click, and remain skeptical of any messages that contain random links or attachments.

Use strong, unique passphrases for each account.

A strong passphrase is a group of words that is easy for you to remember but hard for others to guess. And by creating unique passphrases for each account, you prevent criminals from performing an attack known as credential stuffing—the automated use of breached usernames and passwords to gain fraudulent access to additional accounts.

Respect the access you've been given.

Access refers to the digital and physical clearance our organization has granted you. Respect that access by never revealing your login credentials to anyone, by preventing anyone from piggybacking off your badge or keycard, and by ensuring secured areas remain secure.

Limit what you share.

Spear phishing attacks—those that target specific people—often begin with the scammer mining information about their target from public forums such as social media. The more you share with the public, the more potential there is for you to become a target. Consider setting your profiles to fully private, and only connect with people you know in real life.

KNOW THE DIFFERENCE

Security Event vs. Security Incident

An event, according to the National Institute of Standards and Technology, is "any observable occurrence in a system or network." Security events don't always result in breaches (such as a computer crashing), but could still threaten the integrity of an organization's IT infrastructure.

A security incident is a violation of security policies or standard security practices, which results in negative consequences. Incidents can include someone clicking on a phishing link, or a cyber attack that disables our systems and networks.

Why does this matter? Our organization encounters events daily. An employee receiving an email registers as an event (the email has cleared our spam filters and firewalls). If it's a phishing attack, it doesn't become an incident until someone clicks! It's your responsibility to ensure events don't become more serious.