By Boaz Fischer on Aug, 18 2016

IF YOU ARE INVESTIGATING AN 'INSIDER BREACH'... YOU'RE TOO LATE!

Download & read full article

The difference between an ‘Investigator Team’ and ‘Insider Threat Team’

According to CERT-US, a security incident is the act of violating an explicit or implied security policy according to NIST Special Publication 800-61. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations.

These include but are not limited to:

- Attempts (either failed or successful) to gain unauthorised access to a system or its data
- Unwanted disruption or denial of service
- The unauthorised use of a system for the processing or storage of data changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Security incident response has become an important component for organisation programs. Cybersecurity related attacks have become not only more numerous and diverse but also more damaging and disruptive.

Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented.

And despite organisation being proactive and implementing security measures to ensure the protection of their key assets, no one is immune to a security breach.

Now what?

The typical first step in reacting to a breach is to determine what caused the breach in the first place. This is where an “investigator” steps in to the picture. The purpose of the investigator is to establish the cause so that one can rectify the issue and not let it happen again. Once it has been addressed, organisations can implement an action plan to deal with preventing it from happening again.

Investigators can also be used to investigate “suspicious” circumstances or for a need for a deeper in depth view of the situation.

Now here is the challenge. In my many discussions with a number of the large enterprise organisations, I have often asked them whether they have an Insider Threat Program Manager in place. The usual response is:

“No, I don’t…. But I have an investigation team”

That’s great. It’s the first step, important and critical but one that does not focus fully on potential mitigating Insider Threats within an organisation.

So what is the difference between having a security investigator as part of your team and having an Insider Threat Team?

Let’s define what and “Investigator” role is:

Investigators work at times under difficult and confidential circumstances, they must have the ability to work with, interact with, question and report to all levels of the organisation while maintaining integrity and following prescribed investigation methodologies capable of court challenge. The investigator's role is critical to the company when faced with a security breach or suspects a violation of laws against its own policies &

Latest Posts

Nov, 10 2020
When It Comes To Security Simplicity Is Always Better Than Complexity
Sep, 17 2020
The Risks Of Employee Layoffs And What You Can Do About It?
Jun, 1 2020
The Five Biggest Fallacies About Intellectual Property Theft

Resources

Our experts show their knowledge and insights.

Blog | Articles | Download the Book

About the author

Boaz Fischer is the CEO and founder of CommsNet Group and a recognised leader in promoting and addressing security best practices, awareness and governance. Boaz has written over 50 security articles that are freely available online that with security trust, cloud, mobile, social media and much much more.

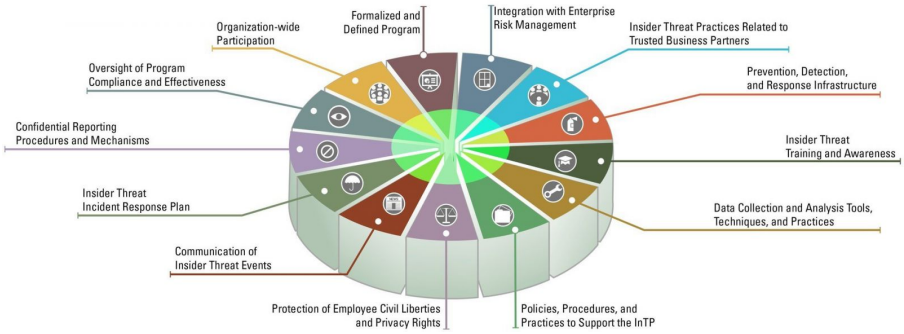
regulations.

Let’s define what an Insider Threat Program is:

The key components of an Insider Threat Program are necessary to prepare organisations for handling insider attacks in a consistent, timely, and quality manner.

CERT Insider Threat Centre have identified a set of key components necessary to produce a fully functioning insider threat program. The full set of components for a successful insider threat program are illustrated in the figure below:

CERT Insider Threat Center Key Components of an Insider Threat Program



An Insider Threat Program provides a robust, repeatable set of processes that the organisation can use to prevent or detect suspicious activity and to resolve malicious incidents.

The benefits of a formalized Insider Threat Program include but are not limited to

- Providing methods for identifying individuals who may be at greater risk to harm the organisation’s critical assets
- Mitigating and controlling damages before they occur
- Helping the organization to conduct triage on the incident and recover as quickly as possible
- Providing methods that detect both intentional and unintentional insiders.

As such an Insider Threat Program provides organisation with a focused method for gaining a deeper understanding of

- What constitutes an Insider Threat
- How to spot the signs of an Insider Threat
- How to protect itself from the devastating consequences of malicious insiders
- The program vets any leads about suspicious activity
- Provides ongoing training
- Handles incidents consistently and effectively

By and large an “Investigator” is only one of the key pieces of an Insider Threat Program. However, an investigator is usually brought in once an incident has occurred, AFTER the breach.

The real difference, an Insider Threat Program Manager is designed to be proactive to mitigate Insider Threats BEFORE they happen.

To effectively mitigate the potential of an Insider Threat to your organisation, it is highly recommended that you develop and implement an Insider Threat Program Framework with a Program Manager.

Find out more

CommsNet Group offers training courses and workshops designed to help organisations learn more about reducing the risks associated with Insider Threats.

- What is insider Threat and How it is different to External Threats
- Insider Threat Workshop – What your organisation needs to protect and the steps to take to prevent Insider attacks.
- How to Increase Visibility within your Organisation to Deter Monitor and Detect Insider Threats
- How to properly Implement an Insider Threat Program in your organisation

CommsNet Group is the only organisation in APAC certified by Software Engineering Institute (Carnegie Mellon University - http://www.cert.org/insider-threat/) .
We can certainly help your organisation effectively implement an Insider Threat Program Manager.

Please contact us on either of the following to setup a time that can discuss your situation

- Email: InTP[@]commsnet.com.au
- Phone: +61 2 6282 5554