Cybersecurity Trends for Today's Support Teams

ONPAGE

Table of contents

Executive Summary

It is absolutely crucial for MSP organizations to establish cybersecurity safeguards and ensure that their client's sensitive data and information remain protected. However, as technology and threats continue to evolve, teams must be reevaluating their cybersecurity measures to align with today's cybersecurity trends and safety measures.

This way, MSPs and support teams can continue to satisfy their stakeholders while retaining valuable clientele as they see the cyberspace expand and improve. Because as much as advancements help us with efficiency, cybercriminals can just as easily utilize these features to create threats that are harder to detect and eradicate.

This eBook discusses the current state of cybersecurity operations, highlighting emerging threats and solutions to these malicious activities.

Cybersecurity Challenges

Michael Zboray, Gartner's former chief information officer and OnPage's current information and cybersecurity advisor, states that the Internet of Things (IoT) poses the greatest cybersecurity threat to today's organizations.

Through the increased connectivity and interaction between devices, sensitive information becomes even more susceptible to breaches and malicious threats.

Additionally, Michael suggests that support teams and MSPs need to better solidify the confidentiality, integrity, and availability (CIA) of information. At its core, CIA ensures that only the right people receive and share accurate, trustworthy information.

Concerning IoT Statistics

Per the Ponemon Institute, breaches rose up to 26 percent in 2019, up from **15 percent** in 2017.

Worse yet, only **nine percent** of organizations are educating their teams about IoT devices and their susceptibility to malicious activity. This contributes to the ever-increasing nature of IoT-targeted attacks.

Additionally, IoT devices tend to go **unpatched** and are often set up with weak credentials or passwords.

Dangers for CIA Triad

Confidentiality, integrity, and availability create the “CIA Triad,” ensuring that sensitive information remains protected and secure. Essentially, solidifying the CIA triad equates to robust data security operations.

However, as the volume of information increases, it often becomes difficult for organizations to protect every data entry or critical detail. Put simply, responsible data oversight becomes difficult when there’s an abundance of data to be responsible for.

This is why MSPs must stay vigilant and consistently research changes and advancements within the cybersecurity industry, actively prioritizing investments in security measures that will improve CIA and align with their organization’s goals.

Real-World Example: Target Corporation

Target Corporation is infamously recognized for its cybersecurity breach in 2013, impacting **40 million** credit and debit card numbers.

Target failed to establish sound cybersecurity practices. For instance, the company **didn't investigate security warnings** (i.e., alerts) forwarded by their cybersecurity experts in Bangalore.

Additionally, the company didn't segment and segregate their systems, which further impacted the retailer and its customer data.

Cybersecurity Solutions

Enhancing cybersecurity operations requires the segregation of IoT devices and information systems, providing a layer of protection for sensitive information in the process. This way, a single data breach cannot fully infiltrate an MSP or IT support organization and its important client records.

Additionally, organizations need to better solidify the CIA triad. For instance, **confidentiality** can be enhanced through access restrictions and promoting password best practices. **Integrity** can be improved through data consistency and data change detection, while **availability** requires constant maintenance of software and hardware systems. Having a sound disaster recovery plan complements these software and hardware upgrades.

Adopting an Incident Alert Management Solution

An incident alert management platform such as OnPage, enhances cybersecurity operations through SSL encrypted communications, ensuring that support team messaging is protected. This encryption extends to in-transit and at-rest communications.

These solutions offer distinctive credentials (i.e., passwords and platform IDs) and SSO integrations for increased user security. Strict password requirements and limited log in attempts heighten the level of security.

Additionally, intelligent alerting solutions (e.g., OnPage) are fully compliant with data security regulations and guidelines for both MSP and IT professionals.

At its core, incident alert management platforms are designed to comply with the most common regulations such as HIPAA, while providing intelligent, persistent alerts during critical situations.

About OnPage

OnPage's award-winning incident alert management system for IT, MSP and healthcare professionals provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. OnPage enables organizations to get the most out of their digital investments, so that sensors, monitoring systems, and people have a reliable way to escalate urgent communications to the right person immediately.

OnPage's escalation, redundancy, and scheduling features make the system infinitely more reliable and secure than emails, text messages and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response times.

Whether to minimize IT infrastructure downtime, or to reduce the response time of healthcare providers in life-and-death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notification needs.

Contact Us For more information, visit www.onpage.com or contact the company at sales@onpagecorp.com or at (781) 916-0040