Cybersecurity Trends for Today's Support Teams

About This eBook

Regardless of the calendar year, it's crucial for IT support teams and MSP organizations to establish cybersecurity safeguards, ensuring that sensitive data and information remain protected.

This way, MSPs and support teams can continue to satisfy stakeholders while retaining valuable clientele.

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

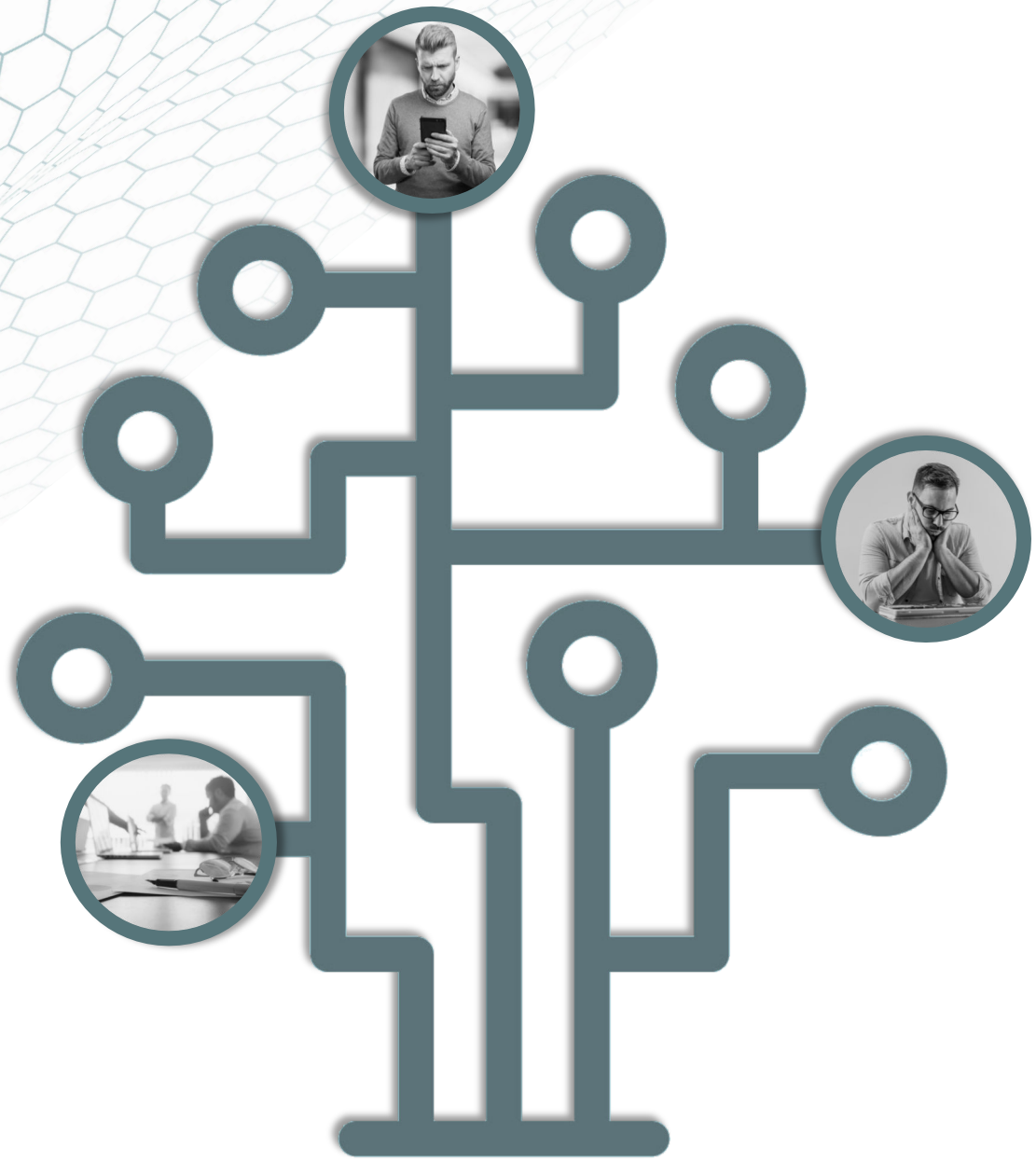
2019 Cybersecurity Challenges

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 connectivity of 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.

Michael Zboray,
information and cybersecurity advisor,
OnPage Corporation



Concerning IoT Statistics

Per the Ponemon Institute, IoT-related data breaches **rose up to 26 percent** in 2019, up from 15 percent in 2017.[1]

Worse yet, only **nine percent** of organizations are educating their teams about IoT devices and their susceptibility to malicious activity.[2] This contributes to the ever-increasing nature of IoT targeted attacks.

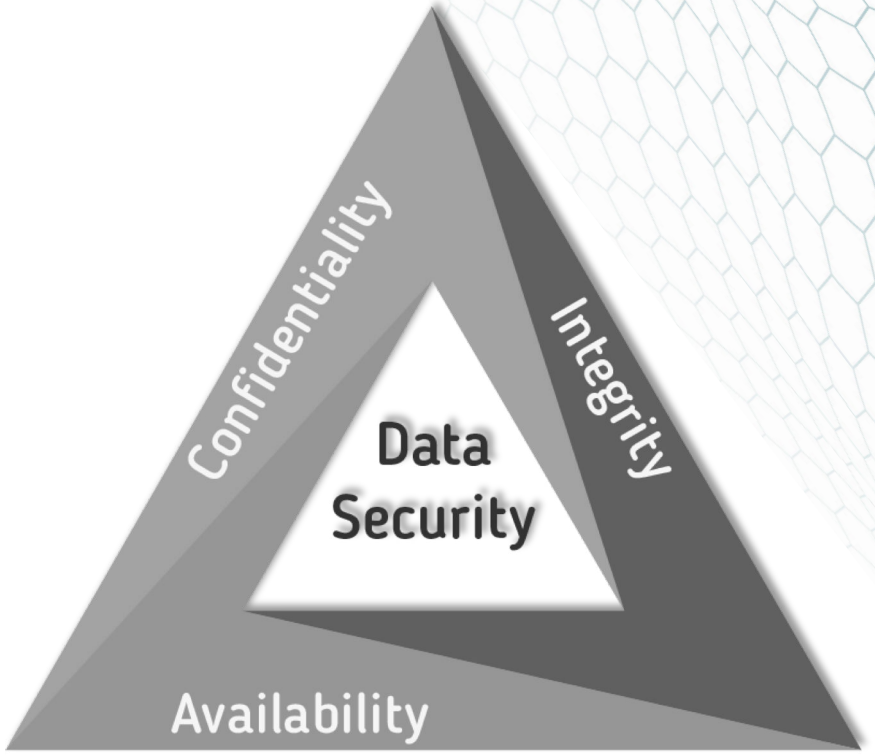
Additionally, IoT devices tend to go unpatched and are often set up with weak credentials or passwords.[3]

1 https://www.businesswire.com/news/home/20190507005347/en/Ponemon%E2%80%99s-Annual-Study-Party-IoT-Risk-Companies/?
2 https://www.channelfutures.com/mssp-insider/iot-attacks-on-the-rise
3 https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Dangers for CIA Triad

Confidentiality, integrity and availability create the “CIA triad,” ensuring that sensitive information remain 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.[4]



4 https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Real-World Example: Target Corporation

Target Corporation is infamously recognized for its cybersecurity breach in 2013, impacting 40 million credit and debit card numbers.[5]

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.[6]

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

5 https://arxiv.org/pdf/1701.04940.pdf
6 https://www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712

Cybersecurity Solutions

Enhancing cybersecurity operations requires the segregation of IoT devices and information systems, providing layers 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 password best practices.[7] 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.

7 https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

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) for increased user security. Strict password requirements and limited log in attempts heighten the level of security as well.

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.

OnPage's award-winning incident alert management system for IT professionals provides the industry's only ALERT-UNTIL-READ notification capabilities. Built around the incident resolution lifecycle, OnPage helps teams reduce downtime and costs while improving coordination and performance.

OnPage's escalation, redundancy and scheduling features ensure that a critical message is never missed. Infinitely more reliable and secure than emails, text messages and phone calls, OnPage provides instant visibility and feedback on alerts. As part of IT service management, the solution tracks alert delivery, ticket status and responses, delivering complete audit trail reporting during and after each incident.

To learn more, contact OnPage at
sales@onpagecorp.com, call (781) 916-0040
or visit www.onpage.com