Thought leadership
White paper

Key considerations to protect your IT infrastructure from ransomware attacks

Ransomware attacks represent an escalating threat for every organization, regardless of size or sector.

What is ransomware?

Ransomware is a form of malware that is designed to block system access until a fee is paid, these cyber attacks can be especially dangerous to small- and medium-sized organizations who often lack the security budgets, IT personnel and expertise of their enterprise-level counterparts.

Properly safeguarding against ransomware strikes has never been more critical. In 2020 alone, the prevalence of ransomware attacks in the U.S. skyrocketed by 109 percent, according to the **2020 SonicWall Cyber Threat Report** costing businesses **more than $75 billion a year**, part of which is attributed downtime expenses.

Experts attribute the rapid increase of threats to the influx of home-based employees resulting from the COVID-19 pandemic. In this new hyper distributed IT environment, the threats are everywhere and should not be ignored.

With increasingly savvy and opportunistic attackers out in full force, you need every possible advantage to ensure your organization is properly protected, including your power infrastructure. In this paper, you will discover how power infrastructure represents a potential point of entry for ransomware attacks and the measures that can be implemented to keep cyber criminals from invading your systems.

The cost of threats are steep

In 2020, businesses are paying more than **$75 billion** a year[1]

Ransomware downtime costs a business an average of **$8,500** per hour[2]

Powering Business Worldwide

[1] Brunau, C. (2021, January 11). **American SMBs Lose $75 billion a year to Ransomware**
[2] Bisson, D. (2020, August 19). **6 Ransomware Trends You Should Watch for in 2020**

Critical cybersecurity tip

It's important for organizations to utilize an enterprise-grade security suite to protect their infrastructure. Businesses must keep their applications, operating systems and firmware up to date, as vulnerabilities are continually being uncovered by hackers. Applying security patches in a timely manner is critical to avoiding attacks.

How power infrastructure is vulnerable to a ransomware attack

If you're wondering why your uninterruptible power systems (UPSs) and other critical power infrastructure need to be cybersecure, consider this: in 2013, attackers used a vulnerability in a Target HVAC unit to steal data on 40 million debit and credit cards belonging to customers of the retail giant.

While many companies hadn't previously considered power infrastructure as a potential point of vulnerability, the Target hack underscored the importance of safeguarding **UPS systems**, power distribution and cooling systems against these determined threat actors. As hackers continually attempt to overcome the cybersecurity mitigations businesses are putting in place, organizations must ensure that there is no point of access for malicious hackers through their connectivity products.

The Eaton Gigabit Network Card

The first UPS connectivity device to meet the UL 2900-1 cybersecurity standard, the **Eaton Gigabit Network Card** (NETWORK-M2) safeguards against possible ransomware attacks, transforming an Eaton UPS into an enterprise IoT device with a focus on cybersecurity.

By default, only essential services run on the network card and all communication is encrypted and certificate-based. The firmware itself is encrypted, preventing attackers from analyzing its structure. Furthermore, the firmware file is signed, making it impossible to apply altered or corrupted versions of the firmware to the card. For an additional security measure, access to the network card requires authorization credentials and all users are assigned role-based permissions based on their required level of access.

Companies can bullet-proof their power infrastructure through the Gigabit Network Card's enhancements for UL 2900-1 and IEC 62443-4-2 certifications. The card's processor also supports stronger encryption, as well as configurable password policy and X.509 Public Key Infrastructure. This card delivers turbocharged speed with Gigabit Ethernet while also enabling organizations to future-proof their platform through the modern system on a chip architecture.

Eaton continually evaluates ongoing information security threats and security patches to the network card and firmware is released in a timely manner to ensure protection. The cybersecurity health of a business is only as strong as its weakest device and the Gigabit Network Card will be one of the strongest links in the chain of protection.

Business continuity planning is a must

Successful organizations not only utilize the previously discussed mitigations to prevent becoming a victim of **ransomware**, but also have a comprehensive business continuity plan in place. The first step is to make sure that files are regularly backed up. In some cases, this simple process will allow victims to recover their data at no cost.

It is possible that ransomware attackers will attempt to coerce a company to pay the ransom by threatening to publicly release sensitive information. For this reason, organizations should always encrypt their data to prevent attackers from gaining this type of leverage. It is also possible for ransomware attackers to encrypt or destroy backups. Because of this, it is essential to maintain a copy of backups in a separate location that is isolated from your network as a last line of defense.

Organizations may also wish to deploy an "air gapped computer," a security measure to ensure that a computer network is physically isolated from unsecured networks, including the internet and local area networks. The goal of a physical air gap is to secure sensitive information to block a **cyber attackers** ability to get their hands on it.

Eaton Intelligent Power Manager (IPM) as an air gap

Although primarily developed to monitor and manage UPSs—as well as gracefully shut down loads during a loss of utility power, even in virtualized environments—**Eaton Intelligent Power Manager** (IPM) software has proven to be an inexpensive, highly viable air gap solution. The software offers a cost-effective way to automate common IT tasks and schedule cybersecurity air gaps to minimize the attack surface area of your infrastructure.

IPM installs easily on Windows operating systems, automatically discovering and monitoring common power infrastructure and IT equipment, and integrating natively with common virtual environments such as, Acropolis, vSphere and HyperV. Working in conjunction with a UPS and/or **power distribution unit (PDU)**, IPM can trigger specific actions on a customized schedule. IPM has the capability to gracefully shut down the replication server, making it completely inaccessible during normally idle time periods. In addition, IPM can completely isolate the replication server from the rest of the network by gracefully shutting down the connecting network switch. When it is time to begin the replication job, IPM will automatically restart the network switch and replication server by cycling the PDU outlets that provide power to these devices. IPM can also ensure that the data backups on the replication server remain safe during a power outage by gracefully shutting down the replication server when the UPS batteries reach a predetermined threshold.

For more information on how to implement a cybersecurity air gap, please refer to this **application note.** In addition, to learn more about how one company used IPM to bolster security through an air gap solution, read the **Grandeur Housing success story**.

Eaton's approach to cybersecurity

Eaton understands that today's customers require a multi-pronged approach to cybersecurity in order to minimize the threat of operational downtime, data loss, and impacts on lifecycle costs and brand reputation. Because cybersecurity incidents can cripple an organization in minutes, customers need suppliers who are willing and able to provide evidence that the products they sell comply with industry cybersecurity standards. Visit **Eaton's Cybersecurity Center of Excellence** for details on Eaton's approach to cybersecurity standards.

While ransomware attacks are a mounting threat across every business landscape, they are especially risky to small- and medium-sized organizations who tend to have smaller security budgets and less IT personnel/expertise. By deploying simple measures, companies can effectively safeguard their IT infrastructure against these expensive and detrimental attacks.

For more information on cybersecurity visit
Eaton.com/cyberdefense

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP152024EN / GG
April 2021

Follow us on social media to get the latest product and support information.

Powering Business Worldwide