aunalytics

Lowering Cybersecurity Insurance Premiums with Managed Security Services

By: Katie Horvath, CMO Aunalytics

A range of factors, driven in part by the COVID-19 pandemic, accelerated by the work from home (WFH) trend, and exacerbated by the Russia-Ukraine conflict, has caused midmarket organizations to receive a high number of cyberattacks that put every organization at great risk. As a result, a greater number of IT professionals are apprehensive as the threats seem to be coming from every direction. Their concerns are justified as these threats, especially those involving ransomware, are occurring at a much higher rate than has been seen in the past.

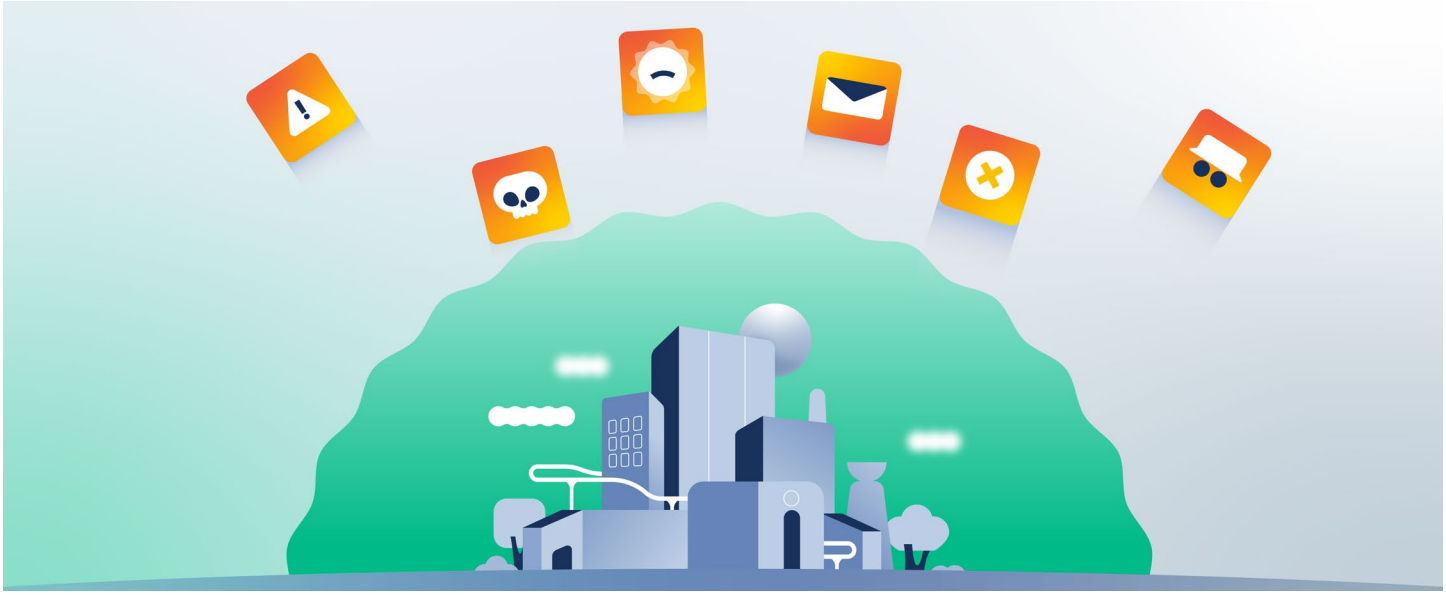
In a March 21, 2022 statement, President Joe Biden cautioned businesses in the private sector to harden their cyber defenses, reiterating earlier warnings related to potential cyberattacks against U.S. organizations by Russia.

"I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners," Biden said. "It's part of Russia's playbook. Most of America's critical infrastructure is owned and operated by the private sector, and critical infrastructure owners and operators must accelerate efforts to lock their digital doors."

> "Most of America's critical infrastructure is owned and operated by the private sector, and critical infrastructure owners and operators must accelerate efforts to lock their digital doors."

- President Joe Biden

Prior to COVID-19 or the Ukraine conflict, IT and security professionals were relatively confident that corporate information was secure as employees primarily accessed their computing devices on-premises—in their offices via their workstation or desktop. However, with a large number of employees now working from home



and receiving some of the spillover attacks from the conflict, many more systems are being successfully compromised as unsecured systems connected through consumer-class Internet providers easily fall to the onslaught of attacks.

One of the biggest threats to impact businesses has been phishing-based ransomware infiltrations which have resulted in $US billions in losses from either paid ransoms or lost business revenues. This is because ransomware is a malware that employs encryption to hold an organization's data for ransom and in an encrypted state, preventing the use of databases and other mission-critical applications. Ransomware also prevents employees from accessing files critical to conducting business operations. Once ransomware enters the network through an employee endpoint, it typically spreads throughout the network, targeting file systems, data repositories of every kind, backup data and more—rapidly taking down the organization.

With the threat of significant financial loss, many midsize businesses are ramping up their security defenses and protecting corporate assets with cyber insurance in the event of a successful attack. Similar to other insurance categories, cyber insurance offers data breach insurance that helps a company to recover from a data loss event due to criminally encrypted data, cyber theft, a network outage, or other IT interruption caused by ransomware, malware or other cyber variants targeting the business.

While larger businesses have been the notable victims of ransomware for years, attacks on midsize organizations are increasing and resulting in major financial losses caused by operational downtime and reduced revenues due to system outages. These attacks have also damaged reputations and resulted in rising costs due to investigations, remedies and other fees or penalties tied to compliance violations resulting from such attacks. With cyber insurance, these businesses can protect themselves from financial losses by not having to pay reparations to criminal entities due to cyber extortion. It also allows companies to be compensated for lost business opportunities and remediation of lost or damaged digital assets.

While cyber insurance is a must-have in today's business climate, it does come with a cost. The often expensive premiums are due to the high compensation required when these attacks occur. Companies in certain verticals such as financial services and healthcare often pay even higher premiums because of the large volume of PII (Personally Identifiable Information) targeted by the most aggressive ransomware or cyber variant.

> "While cybersecurity insurance is the new normal for risk averse organizations, the monthly premiums can be tempered significantly by implementing the appropriate processes and procedures, employee training and robust security infrastructure to defend the organization."
>
> *- Jeff Meyers, VP of Operations for Meyers Glaros*

According to Jeff Meyers, VP of Operations for Meyers Glaros, an Indiana-based insurance firm and provider of cybersecurity insurance, "The cybersecurity threat is something that hangs over every company in America, but more recently has been impacting midsize businesses. While cybersecurity insurance is the new normal for risk averse organizations, the monthly premiums can be tempered significantly by implementing the appropriate processes and procedures, employee training and robust security infrastructure to defend the organization."

The first step to reducing cyber insurance premiums is to conduct a security audit that assesses which digital assets and physical operations may be impacted by an attack. High value and sensitive data ranks number one in these audits with financial data, customer information, employee records, intellectual property (IP) in the form of solution designs/architectures, proprietary processes, strategic plans and more. Once the audit is complete, the calculation of insurance needs can be based on this newly obtained information that determines the potential financial risk and anticipated recovery costs.

The next several steps involve the solicitation of a managed service provider, specializing in secure solution delivery. This includes service providers capable of conducting scheduled penetration testing; business-wide password implementation, monitoring and management; end-to-end encryption of personally identifiable information (PII); deployment of zero-trust infrastructure to control access to sensitive data, as well as a full suite of defensive security solutions layered across the managed IT environment.

Key solutions and processes many insurers suggest implementing to reduce premiums include:

- **Strong email security** - Despite popular belief, email is not a secure form of communication, and every organization should use caution when sending or verifying sensitive information by email.

- **Multi-factor authentication** - MFA immediately increases your account security by requiring multiple forms of verification to prove your identity when signing into an application. Start with your email, then apply MFA everywhere it's available.

- **Full data backups** - A full data backup can mean the difference between a complete loss and a complete recovery after a ransomware attack. Develop a strategy tailored to the business.

- **Secure remote access** - Remote work is more necessary than ever before, which means workers are no longer in controlled work environments. Instead, they are often given access to company resources remotely. When remote access is allowed, the organization takes on additional risks.

- **Regular software updates/patching** - All software presents at least some risk to the organization. Cybercriminals look for vulnerabilities, which can easily be located to prevent exploits through regular software updates.

- **Use of a password manager** - Password managers help keep track of multiple passwords and generate new ones at random. They are essentially an encrypted vault for storing passwords that are protected by one master password. These master passwords act as 'keys to the kingdom' and should be heavily protected.

- **Malicious software scanner** - Endpoint detection and response (EDR) tools (including traditional antivirus and anti-malware software) readily identify, detect, and prevent advanced cyber threats.

- **Data encryption** - Encryption is a process that renders data inaccessible to bad actors who manage to steal it unless they possess the key required to access it. If your data is not encrypted and you lose a device, your organization may face a data breach and all of the legal, regulatory, and notification costs that come with it.

- **Security awareness training** - 60% of claims are the result of human error. This can be avoided by creating a culture of cyber risk awareness that holds everyone accountable.

- **Oversight by a managed IT help desk** – Insurance providers understand that attacks occur at all hours of the day and night. A 24/7/365 help desk monitors security infrastructure and can take action immediately once an attack is detected.

With the combination of secure managed IT services and the right cybersecurity insurance provider, organizations can significantly reduce the threat of serious business and financial impact caused by a successful cyberattack. With critical IT systems, data, and processes in a hardened defensive position, insurance premiums can be made much more affordable while still offering all-encompassing protection against the criminal threat actor's incessant flood of attacks. Even more important, with a secure managed services contract in place, successful attacks are made incredibly difficult for even the most experienced cyber villains—dramatically reducing the risk profile of the organization.

About Aunalytics

Aunalytics is the data platform company delivering answers for your business. Aunalytics provides Insights-as-a-Service to answer enterprise and midsized companies' most important IT and business questions. The Aunalytics® cloud-native data platform is built for universal data access, advanced analytics and AI while unifying disparate data silos into a single golden record of accurate, actionable business information. Its Daybreak™ industry intelligent data mart combined with the power of the Aunalytics data platform provides industry-specific data models with built-in queries and AI to ensure access to timely, accurate data and answers to critical business and IT questions. Through its side-by-side digital transformation model, Aunalytics provides on-demand scalable access to technology, data science, and AI experts to seamlessly transform customers businesses. To learn more contact us at +1 855-799-DATA or visit Aunalytics at https://www.aunalytics.com or on Twitter and LinkedIn.