WHITE PAPER

CYBERSECURITY WAKE-UP CALL:

A 6-STEP APPROACH TO PRO-ACTIVE INCIDENT RESPONSE CAN AVOID CATASTROPHIC RESULTS FOR BUSINESS

Business has a new battleground. The foes aren't competitors, but they are silent intruders beating at the doors of virtually every organization. They are cyber-criminals seeking to steal valuable or private data, extort money, impair the operation of a business or simply create havoc. The costs of security breaches often reach the millions of dollars.

As much as today's always-connected, highly-mobile, data-intensive world is a boon for business, it is also a fertile breeding ground for cyber-criminals. Techniques such as malware attachments, drive-by downloads, distributed denial-of-service (DDoS) attacks, ransomware, keyloggers and screen grabbers, along with social engineering tactics such as phishing are increasingly commonplace.

Yet these breaches often catch businesses completely by surprise, regardless of what may appear to be sophisticated approaches to cybersecurity. And too many organizations lack an effective response when a cyber-attack does occur.

The answer? No network or device can be impervious to attack, but the best protection stems from an intelligent approach to the incident response lifecycle, from preparing defenses to effective remediation strategies to constant learning and improvement.

EXPLODING THREAT LANDSCAPE

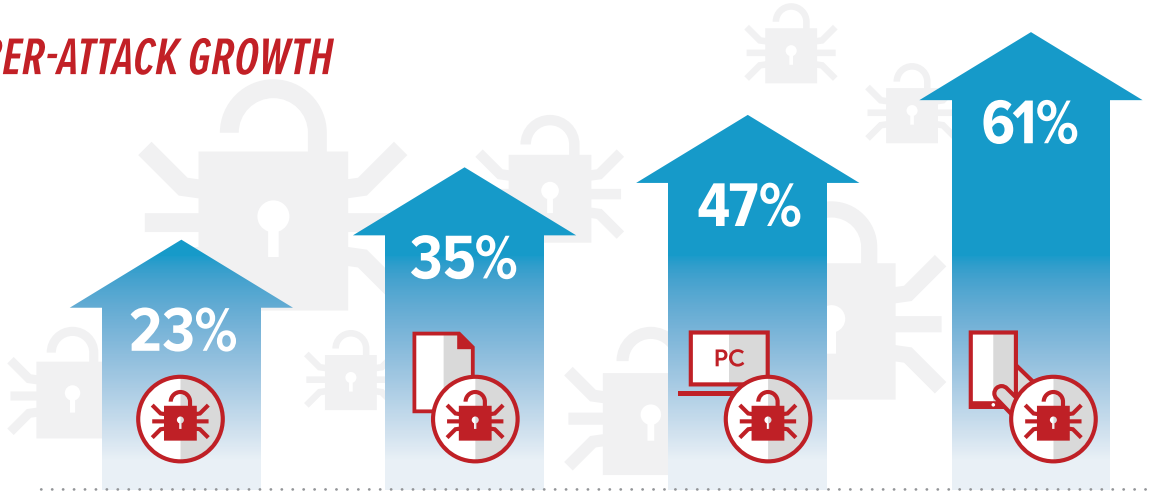
There is no question about the potential damage that can be caused by a malicious attack on an organization's network or connected devices. For example, interference with medical information systems and devices can affect lives; an organization's communications can be compromised; financial transactions can be disabled or large amounts of money stolen; businesses can be literally brought to a halt – the list of possible negative or even dire consequences goes on and on.

Research suggests that the cyber-criminals are extremely effective. A recent survey of businesses found that 45.5% had been impacted by a security incident during an average month.[1] In another global survey, 46% of nearly 3,000 business leaders believed there was a medium likelihood of a cybersecurity attack disrupting electrical, water or other critical infrastructure this year. An additional 38% believed there was a high risk of such an attack.[2]

The explosion of mobile devices, cloud apps and virtualized servers have compounded the threat by expanding the attack surfaces open to potential attackers. The fast growth of IoT (Internet of Things) devices is expanding the threat landscape as it creates networks of interconnected data collection and processing devices that often lack adequate security, and are therefore ripe for exploitation by attackers.

So it's no surprise that the numbers of security threats and incidents are growing incrementally. This chart shows the startling growth of various kinds of cyber-attacks.

CYBER-ATTACK GROWTH



Malware
The total number of malware samples grew 23% in the past year to almost 723 million.

Macro Malware
New macro malware rose by 35% in just one quarter, raising the total count to 1.1 million.

Ransomware
New ransomware samples grew 47% in the past year to 10.7 million samples.

Mobile Malware
Infections by mobile malware grew 61% in the past year to 18.4 million samples.

Statistics from McAfee Inc. for Q2 2017 • http://www.mcafee.com/September2017ThreatsReport

Yet even in the face of growing numbers of threats, Canadian companies have been relatively slow to prepare for the advent of a cyber-attack. For example, of Canadian companies hit with a ransomware attack over a recent 12-month period, fully 75% of them were forced to pay the ransom to restore their data or systems. Compare this with the U.S., where only 3% of companies were forced to pay.[3]

Given these active threats to today's data-driven businesses, safeguarding networks and data has become one of the most significant challenges facing organizations. Planning and implementing an effective Incident Response strategy has become imperative for all businesses, regardless of size of the organization, or amount invested in security in the past.

A recent survey of businesses found that 45.5% had been impacted by a security incident during an average month.[1]

6-STAGE APPROACH TO PRO-ACTIVE INCIDENT READINESS AND RESPONSE

Ask yourself ... Are we fully protected against a ransomware, data breach or other cyber-attack? Are we truly prepared? What plans are in place to deal with an attack, and quickly recover from it?

A pro-active Incident Response Plan is key for organizations to ensure the highest level of protection but, just as important, to recover quickly in case a security incident does occur. Security expert ISA recommends implementing a documented Incident Response Plan based on a 6-stage approach that ensures readiness throughout the Incident Response lifecycle:

1. ***PREPARATION*** **– Review of existing security infrastructure, preparing identification and response plans, and implementation of incident response tools and processes**

Most organizations rely on an expert partner to plan and implement a cybersecurity Incident Response platform. This ensures that all the critical insight and expertise is always available in case of an attack. When choosing a security partner, organizations should look for these characteristics:

+ Proven ability to monitor for security incidents and quickly identify threats, with a proven track record of success.
+ Ability to respond instantly. Experts in this space should be able to respond with initial triage within no more than 30 minutes.
+ Proven processes, tools and techniques to handle security incidents from identification through remediation. When facing a cybersecurity attack, there is no room for error and no time to coordinate multiple service providers.
+ 24/7 threat monitoring and detection, usually with the support of a dedicated cybersecurity intelligence and operations centre.

2. *IDENTIFICATION and ASSESSMENT* – **Timely detection of security incidents and determination of their nature and potential impact.**

An organization's ability to identify and assess a cybersecurity attack (and therefore the ability to fight it) usually depends on the processes, tools and techniques that have been put in place. Without them, a threat, breach or targeted attack might actually go undetected; or if it is detected, it may be impossible to identify its nature, determine the source or attack vector, or quickly assess how to contain and remediate it.

When an attack is detected, so many questions require very fast answers. What is it? Where is it coming from? What damage is it doing, aside from what may be obvious? And most important, what is the best strategy to quickly contain the damage and begin recovery? A clear action plan is required, along with a great deal of insight and expertise.

Where an Incident Response plan is in place, many of these questions can be immediately answered, and the steps through identification, assessment and containment are clearly detailed so they can be implemented quickly and effectively.

3. *CONTAINMENT* – **Immediate action, using documented processes, to limit damage and prevent any further loss or impairment.**

Once the source and nature of a breach or attack is identified, time is truly of the essence to limit damage or loss. Containing the damage may require a variety of tactics at the firewall, network and endpoint levels. Using proven processes, cybersecurity professionals use a variety of techniques and tools (often proprietary ones) to close the attack path and eliminate the ability of the attack to spread, propagate or otherwise continue to cause damage.

4. *ERADICATION* – **Evaluation of systems to ensure the security incident is fully remediated.**

Where a malware or other cybersecurity attack that directly impact networks or devices is neutralized and contained (the persistence or spread is stopped) it must be eradicated from the environment. This is often the most challenging stage of the Incident Response process -- removing all remnants from the environment, and ensuring all attack windows are closed. Many tools and techniques are available to use in this process but, in the case of many types of attacks, it takes professionals with particular expertise and powerful tools to truly clean a system.

5. *RECOVERY* – **Restoration of data and network availability, as well as confidentiality and ongoing integrity.**

Requirements for restoring data and availability depends on the nature of the breach or attack, and extent of the damage. Generally, it is a process of enabling backups or restoring networks. However, if the damage was more extensive, it could require re-installation of software or applications, or re-connection of endpoints to get back to normal operations.

A pro-active Incident Response Plan is key for organizations to ensure the highest level of protection but, just as important, to recover quickly in case a security incident does occur.

6. ***LESSONS LEARNED*** **– Review and assessment of the events and processes that have taken place, and application of improvements to the plan.**

No one wants to suffer a second cyber-attack, no matter the nature or extent of the first one. But regrettably, the best lessons often come from bitter experience. So following a cyberattack, it is important to leverage what has been learned via a thorough review of how the attack happened and the events that took place. Recognizing how and why an attack has occurred, and knowing the points of access and failure points in the system, are key to forming or refining the Incident Response Plan going forward.

PREPARE NOW OR PAY LATER

Virtually any organization is susceptible to malicious cyber-attacks regardless of security posture. The costs of reputational damage, business impairment, financial loss and even lawsuits can be daunting.

It's a matter of taking steps to prepare now, or face those consequences later. This kind of comprehensive, multi-stage approach to the Incident Response lifecycle will ensure the fastest and most effective detection and remediation of any security incident.

If you're interested in how an effective Incident Response strategy can be implemented in your organization, contact ISA at 1-877-591-6711 or visit e-isa.com.

ISA is a security-focused technology firm, with over twenty years of experience helping organizations across Canada solve complex challenges relating to IT security. We act as trusted advisors to help our clients define, implement and manage strategies to minimize IT security risks, and provide a secure business environment for employees and customers. Visit e-isa.com.

[1] Telstra 2016 Cyber Security Report, https://www.telstra.com.au/business-enterprise/campaigns/cyber-security-report
[2] http://www.isaca.org/cyber/Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt_Eng_0116.pdf
[3] Osterman Research 2016, https://www.csoonline.com/article/3101863/security/report-only-3-percent-of-u-s-companies-pay-attackers-after-ransomware-infections.html

CONTACT US

For more information, contact us at:

1-877-591-6711
info@e-isa.com

ISA Inc
isa_inc
ISA

TORONTO (Head Office)
3280 Bloor Street West, Suite 1100
Centre Tower, 11th Floor
Toronto, ON M8X 2X3
Tel: 416-591-6711
Fax: 416-352-7512
Email: info@e-isa.com

CALGARY
144 - 4th Avenue South West
Suite 1600
Calgary, AB T2P 3N4
Tel: 403-695-1790
Fax: 403-716-3637
Email: info@e-isa.com

OTTAWA
1 Rideau Street
Suite 700
Ottawa, ON K1N 8S7
Tel: 613-670-5741
Fax: 613-670-5701
Email: info@e-isa.com

Visit us online at **www.e-isa.com**