Enterprise Cybersecurity – Navigating the Digital Threat Landscape

## The digital age has made the world more vulnerable to cyber-attacks. With modern IT infrastructure extending far beyond traditional data centres, cybersecurity professionals must be on constant alert to navigate the growing threat of cybercrime—before it impacts a company’s data, finances, and reputation.

## A Need for Enterprise Cybersecurity Programs

As more businesses go digital and network boundaries virtually disappear, the threat landscape is harder to manage at the enterprise level. To effectively combat the spread of cybercrime, a robust cybersecurity program must include state-of-the-art technologies, processes, and practices that ensure the confidentiality, integrity, and uninterrupted availability of critical information. A companywide approach is vital to a program’s success since malicious attacks can strike anywhere, at any time—on-premises, in the cloud, and on the go with employees operating multiple devices to do their jobs.

This whitepaper focuses on how to meet cybersecurity challenges across a shifting IT environment, suggesting that managed security services providers (MSSPs) can be of help. A case study highlights the impact of Acronym Solutions’ MSSP expertise, driven by strategic thinking to align with a particular company’s cybersecurity vision. Finally, a roadmap for the deterrence of cyber warfare is presented along with future implications.

## Meeting Cybersecurity Risks & Challenges

Perhaps the biggest cybersecurity challenge is the rapidly changing nature of digital threats. Millions of hackers work around the clock, around the world to develop new cybercrime methods faster than companies can update their defences, so even the most secure network requires rigorous surveillance. The following problems underscore an urgency to invest in innovative, intelligent technological solutions that mitigate security risks.

### The high cost of pervasive cybercrimes

Corporations face an escalating number of cyber-attacks, which are reported to incur increasing financial risks. In 2023, data breaches cost an average of USD 4.45 million per incident—a 15% increase over the previous 3 years. Notably, [IBM’s Cost of a Data Breach Report 2023](https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs?_ga=2.153279728.953359271.1695827083-1742714580.1695827083&_gl=1*d445v6*_ga*MTc0MjcxNDU4MC4xNjk1ODI3MDgz*_ga_FYECCCS21D*MTY5NTgyNzA4Mi4xLjEuMTY5NTgyNzU1MC4wLjAuMA..) revealed that 95% of surveyed organizations endured multiple breaches, and only one-third of organizations detected the breach themselves. The stakes are just as high for smaller-sized entities. [Accenture](https://www.accenture.com/us-en/insights/cyber-security-index) found that small businesses are the target of 43% of all cyber-attacks, with an average loss of USD 188,000 per attack. Recent high-profile cyber-attacks against Canada’s retail, healthcare, and energy sectors are an indication of just how widespread threats have become. No one is immune.

### The shortage of skilled labor

Another significant challenge is finding and hiring an adequate number of cybersecurity experts. The [2022 Cybersecurity Workforce Study](https://www.prnewswire.com/news-releases/isc-research-reveals-the-cybersecurity-profession-needs-to-grow-by-3-4-million-people-to-close-global-workforce-gap-301654730.html) found that more than 3 million additional workers are needed to secure global assets—despite this specialized workforce being at an all-time high. It is troubling that 70% of organizations surveyed say they do not have enough qualified cybersecurity professionals on staff. The high demand and scarce supply scenario drives up IT costs, as well.

### The modern IT environment

Dispersed computing (aka distributed computing) is the new normal for modern IT environments. This makes it more difficult to provide 24/7/365 global cybersecurity coverage that guards against all potential risks—such as data leakage between applications and devices—threatening every IT asset, ranging from smartphones to laptops, servers, and cars. Factor in high volume, complex computing to run AI workloads, and there is a clear need for strict cybersecurity controls, as well as aggressive risk management, to protect ‘zettabytes’ of data.

## What Makes a Successful Enterprise Cybersecurity Program?

### A top business priority

Cybersecurity is no longer confined to the IT department; it permeates every facet of an organization and, therefore, needs to be considered a high-priority business imperative and growth accelerator—topping other pressing matters of the day. This means investing in the latest detection tools to identify security breaches in real time and adopting a proactive mindset to anticipate next-generation cyber threats. For example, enterprises must be aware of and take seriously the looming threats of [organized cybercrime gangs](https://jamcyber.com/blog/cyber-insights/cyber-crimes-gangs/), who are driven by high-priced commissions and think nothing of leveraging world events to create chaos.

### Constant surveillance

Digital transformation has brought the convenience of universal connectivity, enabling business to be conducted from virtually any place workers choose to work. That also means a wider threat surface for cybersecurity surveillance systems to cover, and the need for those systems to constantly monitor all activity, on-premises and in the cloud, to avoid gaps in coverage. For many of the reasons mentioned above, this can be an overwhelming goal for many IT teams to accomplish on their own.

### Moving toward consolidation

A unified enterprise cybersecurity program is sorely needed. Migrating to a consolidated cybersecurity platform is necessary to defeat sophisticated cyber criminals looking for weak links and applying novel methods of intrusion. However, consolidating cybersecurity systems is a complex journey requiring a high degree of technical expertise to properly execute.

### Overcoming obstacles

For a change like this to succeed, certain obstacles must be overcome along the way, such as:

* + - * **Legacy systems** – Existing, standalone software systems may be difficult to integrate with modern IT platforms. Migrating data and functionality from these systems can be time-consuming and error-prone.
      * **Vendor lock-in** – Contracts with existing vendors may make it challenging to switch to new solutions. Negotiating new terms or transitioning away from proprietary tools can be tricky.
      * **Interoperability** – Ensuring seamless communication between different security tools is crucial. Incompatibilities can lead to gaps in coverage or false positives/negatives.
      * **Skill gaps** – Consolidation may require training staff on new tools or processes. A lack of expertise can hinder successful implementation.
      * **Risk of disruption** – Transitioning systems can disrupt ongoing security operations. Organizations must carefully plan and execute the consolidation to minimize downtime.
      * **Budget constraints** – While consolidation can save costs in the long run, initial investments may be substantial. Balancing budget constraints with security needs is essential.
      * **Change resistance** – Employees may resist changes due to familiarity with existing tools. Change management and communication are critical.

## How Managed Security Service Providers Can Help

The ever-evolving threat landscape, combined with the resource shortage, makes partnering with an MSSP a viable solution. According to [IBM’s Cost of a Data Breach Report 2023](https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077724064006&p5=e&gclid=EAIaIQobChMI3tfe2KXNgQMVBpHCCB0Q_wPBEAAYASAAEgKcq_D_BwE&gclsrc=aw.ds), organizations that suffer an attack experience a 21% shorter breach lifecycle when working with an MSSP.

### MSSP value-adds

Think of MSSP as a lifeline, linking you to a highly skilled team of experts and rigorous processes that help you confront cyber threats and bad actors. MSSPs value-adds include:

* Educate you about the current and upcoming threat landscape
* Assist you in developing cybersecurity policies and procedures
* Assess your existing security systems and solutions
* Recommend cost-effective methods to identify gaps and reduce vulnerabilities
* Provide visibility across all your cybersecurity controls

### MSSP benefits

IT departments may opt to supplement their cybersecurity program and core staff by outsourcing specific functions to an MSSP or delegate their entire security operation to the experts. MSSPs provide comprehensive support and leading-edge technologies that deliver the following benefits:

* Increased confidence in your cybersecurity posture
* Access to a wide breadth of flexible and innovative security solutions
* Consolidated security platform, from premises to the cloud
* Innovative security tools, such as threat intelligence, machine learning (ML), artificial intelligence (AI), automation, and big data analytics

## Case Study – Optimizing a Cybersecurity Program for the Flooring Industry

This case demonstrates how Acronym Solutions transformed a company’s cybersecurity program fraught with limitations, taking it to a new level of efficient and effective protection against potential threats.

### Who

## An Ontario-based flooring company that manufactures premium, customized wooden planks, as well as cabinetry, for high-end interiors, commissioned the MSSP services of Acronym Solutions.

### What

The company’s cybersecurity program was underperforming due to slow internet speeds, a lack of IT resources, loose security controls exposing the network infrastructure, no security policy, and no backups in place. These numerous challenges were more than the company could solve on its own; thus, they chose to leverage the augmented staff and experience offered by an MSSP.

### How

Acronym’s MSSP team first assessed the current state of the company’s digital landscape and existing safeguards. Based on their findings, they recommended a tailored solution that bundled certain managed security and IT service offerings and also included Dedicated Internet Access (DIA) in response to a desire for faster connectivity.

#### DIA Solution

Installing DIA served two purposes: 1) the DIA’s private nature meant the company would not have to share an internet connection with other businesses, thereby increasing overall security; and 2) the upgraded internet connectivity from 150Mbps to 1Gbps dedicated fibre provided 6.8 times higher speed, uninterrupted reliable service, low latency, flexibility, and scalability for future growth.

#### Managed Security and IT Services: A Bundled Solution

**Managed firewall** – provided next-generation firewall (NGFW) protection with deeper packet inspection, improved network visibility, integrated threat intelligence, optimized traffic flow, granular policy controls, and consistent enforcement, plus the added benefit of a unified management console for simplified security administration.

**Secure email** – provided a dedicated email hosting service with end-to-end encryption; advanced spam filtering and virus protection against phishing attacks, malware, and unauthorized access; and consistent, reliable uptime.

**Secure endpoint detection and response (EDR)** – provided advanced and early threat detection, rapid response and remediation, enhanced security posture, user and device behavior monitoring, regulatory compliance, detailed reporting, and cost efficiency.

**Secure backup** – provided an office backup appliance to conduct routine, automated backup schedules with data encryption, data redundancy, fast recovery/restoration of data, and a business continuity/disaster recovery plan.

### Outcome

The following business results were a direct outcome of this cybersecurity optimization project:

* Safeguarded the organization's critical data assets
* Implemented an end-user protection policy
* Ensured business continuity (on-premise and cloud backups for quick data recovery)
* Enhanced overall operational performance and resilience

## Contracting MSSP Services – When and Why

### The right time

The company highlighted in the above case study knew it was time to step up its cybersecurity efforts, but it is not always as straightforward. If your organization is experiencing any of the following pain points, it may be time to contract the services of an MSSP:

1. Qualified cybersecurity professionals are in short supply within your organization and in the wider labour market where you operate.
2. You require immediate access to highly trained and knowledgeable experts whose sole focus is on cybersecurity.
3. You want to reduce or eliminate ad hoc technology investments and are looking for a more predictable and cost-effective cybersecurity solution.
4. Time and budget constraints make establishing an in-house cybersecurity program/team impractical.
5. Your organization wants to take a proactive stance in prioritizing threat prevention, instead of just reacting to threats as they arise.
6. It has become necessary to monitor your critical systems and infrastructure 24/7 to reduce the risk of security breaches.
7. Your company requires assistance with navigating complex regulatory frameworks and compliance issues.
8. Your business is expanding to a new jurisdiction and wants to ensure consistent security standards across all locations.
9. Crafting a well-defined cybersecurity incident response plan has become a major corporate focus.

### The right partner

A trusted partner, like Acronym Solutions, can help evaluate your cybersecurity needs and customize a plan that will work today, and scale for tomorrow’s growth. Acronym’s cybersecurity services are designed to provide full protection for business networks. These services may be bundled and integrated seamlessly for layered security, giving you the peace of mind that your IT environment is shielded end-to-end with controls and monitoring technology to detect the most dangerous digital threats.

## Charting a Roadmap for the Future

### Basic security architecture measures

In an era of growing cyber threats, it is critical to optimize the scope and design of your security architecture. The good news is that most cyber incidents can be prevented by implementing four basic security measures:

1. **Consolidate your cybersecurity system** – This requires a software suite of cybersecurity capabilities running on a single platform.
2. **Embrace a prevention-focused model** – This proactively eliminates potential threats before they reach your organization’s network, reducing damages and costs to your business.
3. **Strive for holistic protection** – This involves developing a cybersecurity program that offers comprehensive protection for all potential targets across the broadening attack vector, ranging from individuals to the Internet of Things (IoT).
4. **Leverage MSSP support** – This cost-effective approach bolsters your organization’s defences with outsourced services like security infrastructure setup, 24/7 threat monitoring, vulnerability assessments, and incident response handling.

### New solutions for a new landscape

The [Canadian Centre for Cybersecurity](https://www.cyber.gc.ca/en) claims that ransomware is the most disruptive form of cybercrime facing Canada and warns that such threats will only intensify in the years ahead. An expanded digital landscape opens the door to other powerful tactics, such as AI-driven cyber-attacks, dictating new solutions be developed either in-house or by MSSPs.

Ideally, a modern cybersecurity program would include “smart” automated surveillance systems, advanced analytics, and AI/ML along with traditional security measures (such as network segmentation, access controls, and employee training). Additionally, coordination among cybersecurity professionals, researchers, and policymakers is essential to understand the nature of evolving threats and anticipate the risks posed by future iterations of cybercrime.

### Outsmarting the enemy

As treacherous nation-state actors and opportunistic cybercriminal groups continue to develop advanced cyber weaponry, they will endanger critical infrastructure, government agencies, and other high-value assets. To prevent significant risks to national security and public safety, we need to outsmart and outmaneuver the enemy by meeting attacks with iron-clad defences.

Wherever you are on the path to cybersecurity, each step you take to strengthen controls and hold attacks at bay will help your organization avoid damaging and costly losses. Together, we can win the war.

# Why Acronym

Acronym Solutions offers top-tier cybersecurity solutions designed to protect against today’s evolving threats and secure your digital footprint. [Click here](https://acronymsolutions.com/solutions/security/secure-it/) to learn more about our innovative and cost-effective managed security solutions.