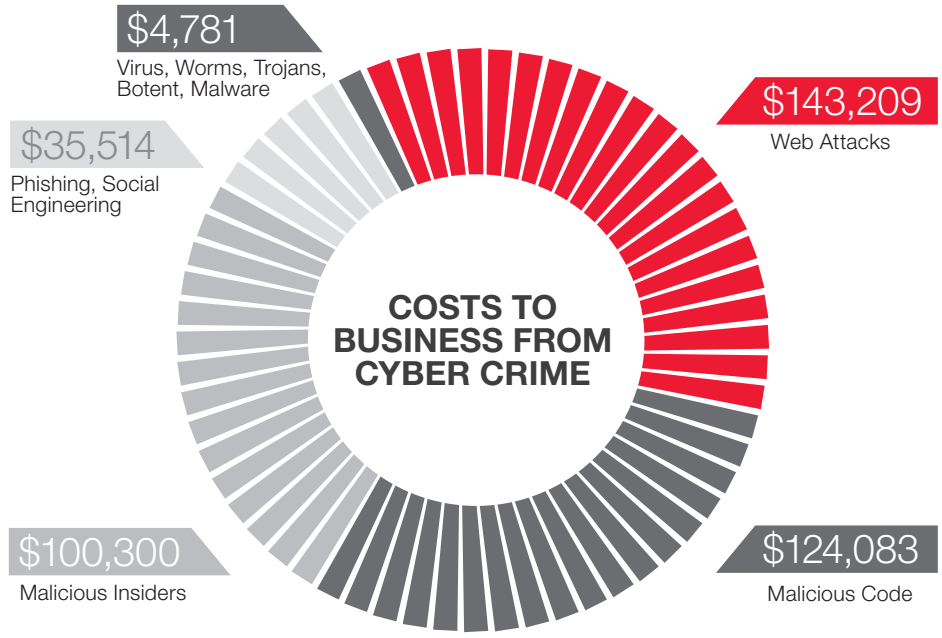
HITACHI
Inspire the Next

MANAGED SECURITY SERVICES (MSS)

THE CYBER SECURITY INITIATIVE

Cybercrime is becoming an important factor for CIOs and IT professionals, but also for CFOs, compliance officers and business owners. The current cyber security threat landscape is getting more and more complex and the decision of buying and implementing solutions to defend against cybercrime can be quite challenging.



Source: Ponemon Institute – First Annual Cost of Cyber Crime Study. 2010

In many cases security requirements have become part of compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and others. Additionally, the cost of cybercrime to businesses is on the rise with the majority of this cost coming from web attacks and malicious code.

Motivations can vary, but cyber security readiness is becoming a must for most organizations regardless of their size or vertical.

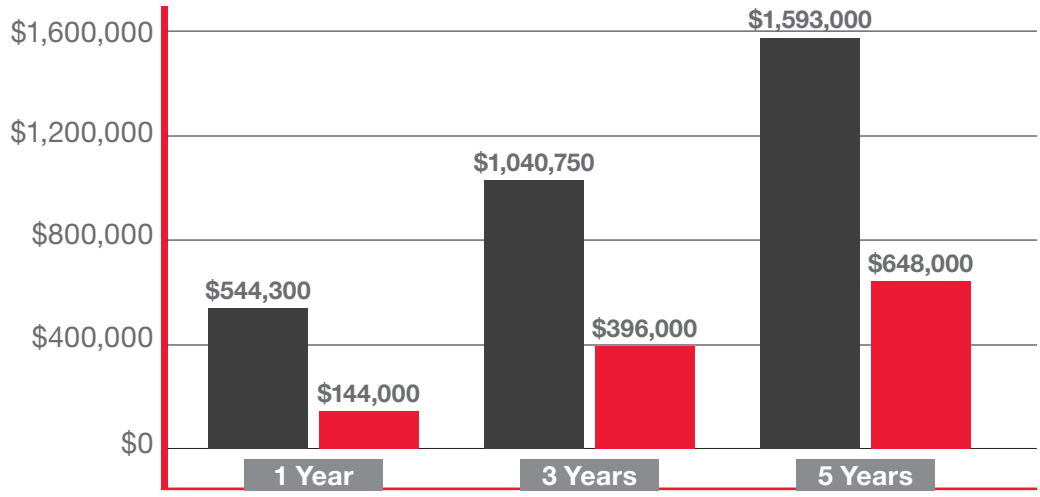
HITACHI SYSTEMS SECURITY INC.'S MANAGED SECURITY SERVICE OFFERING HELPS ORGANIZATIONS

- Detect and prevent cyber attacks
- Manage network and applications vulnerabilities
- Comply with regulations
- Work with security specialists
- Get the best protection possible at a fraction of the cost

THE CASE FOR MANAGED SECURITY SERVICES

The threat landscape is an ever-changing one. Hackers are continuously coming up with new tactics and exploring new vulnerabilities in today's fluid IT environments. While on-premise Security Information and Event Management (SIEM) systems provide a certain level of protection through log collection and management, they require significant in-house expertise and continuous training and education. Staffing can also be challenging, as monitoring critical IT assets on a 24/7 basis requires a high level of specialized staff.

CYBER SECURITY MONITORING COSTS FOR A MEDIUM-SIZED BUSINESS



Outsourcing your security can be a tough decision to make, but for many organizations it makes business sense. Here are a few reasons why you should consider it:

- Staying up to date on the latest security threats can be mission impossible if you don't have dedicated staff for it. Monitoring and protecting your IT assets from cyber attacks is the core expertise offered by Managed Security Service Providers (MSSPs).
- MSSP security expert teams will vet all the alerts produced by the various devices that you may have in your infrastructure to the handful of events that your team needs to deal with, thus reducing cost while increasing efficiency.
- The initial and continuous infrastructure and staffing investment in a security solution can be daunting to some businesses. But even if you can afford that, outsourcing your security services can slash your investment by a significant margin depending on the size of your infrastructure. That should allow you to get the best protection possible and still have the budget to invest in your core business.

STANDARD FEATURES OF HITACHI SYSTEMS SECURITY INC. MANAGED SECURITY SERVICE (MSS) INCLUDE:

THREAT MONITORING – 24x7 monitoring, management and notification of internal and external threats to your organization's network environment insuring optimal protection from cyber attacks at all time.

INTRUSION DETECTION & PREVENTION SYSTEMS (IDS/IPS) – Networks are monitored for malicious activity and policy violations, triggered alerts are analyzed in real time, security incident reports are prepared and security incidents are escalated according to the conditions established in the escalation procedure.

EVENT CORRELATION – Information from a variety of sources, e.g. security logs, vulnerability scans, and IDS alerts, is evaluated to recognize event patterns that may have a bearing on the organization's security posture.

LOG MONITORING – Security-related log data is captured and analyzed in order to identify security incidents, fraudulent activity, and operational problems.

INCIDENT RESPONSE MANAGEMENT – As soon as a security alert is detected, a certified security analyst investigates the alert based on his or her expertise and understanding of the customer's infrastructure. If the alert is determined to be a threat to the customer's network, it will be escalated according to the parameters established in conjunction with the customer.

VULNERABILITY ASSESSMENTS – Vulnerabilities and weaknesses in the network are identified and managed. A variety of network devices, e.g. servers, appliances, applications and workstations, can be scanned for vulnerabilities.

REPORTING – Regularly provided reports are a valuable method to provide customers with more insights on the monitoring service, their security posture, incidents which have been handled since the last report publication, actionable recommendations and general observations and trends about their network.

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada
Tel: +1 450-430-8166 Fax: +1 450-430-1858
www.hitachi-systems-security.com