Deloitte.

The cyber security imperative

Protect your organization from cyber threats

Contents

Cyber threats are real and growing

Corporate espionage. Political activism. Market disruption. Financial gain. Whatever the motivations, cyber crime has become pervasive and continues to spread. From May 2012 to May 2013, Canadian organizations suffered over $5.3 million in losses due to cyber attacks[1] caused by data sabotage, virus and malware propagation, theft of devices, financial fraud and other vulnerability exploits.

Beyond inflicting severe financial loss, cyber attacks can lead to regulatory sanctions, business continuity disruptions, lawsuits and staggering reputational damage.

No business or public sector organization is safe. As cyber criminals become increasingly savvy, organizations often find themselves hopelessly outmatched as their employees', customers' or constituents' private data – from financial records and secure passwords to health information and even identities – falls prey to these concerted attacks.

As industries become more interdependent, the pace of change accelerates and reliance on cyber grows, the potential for catastrophic physical and economic damage mounts. To protect against these cyber threats, organizations need more powerful cyber security solutions – ones that allow them to identify threats in real time, limit exposures, reduce time to recovery and prevent future attacks. Deloitte can help.

A full range of cyber security solutions

While most organizations understand the importance of protecting their systems, networks and data from cyber threats and breaches, it is becoming increasingly difficult to counter these attacks without help. Kennedy Consulting Research & Advisory, a leading analyst firm, recently released a report that addresses this issue. The report provides an assessment of cyber security consulting providers in terms of the relative breadth and depth of their cyber security consulting capabilities. Notably, Deloitte was named a Kennedy Vanguard Leader and identified as the provider with the most comprehensive competency strengths across the cyber spectrum.[2]

Deloitte has honed these strengths by providing security services to some of the world's largest organizations. Globally, we have over 900 Certified Information Systems Security Professionals (CISSP), 1,500 Certified Information Systems Auditors (CISA), 150 Certified Information Security Managers (CISM) and 65 Certified International Privacy Professionals (CIPP). We also have Security Technology Centres located strategically across Canada.

To help organizations realize the benefits of digital business, while mitigating its risks, our cyber security services cover four critical elements:

Sense

To counter cyber security threats, you need to know which threats are relevant to your organization and where they originate. Deloitte's cyber sense capability can help you identify current and emerging cyber threats and address vulnerabilities in your cyber profile.

Related services: Cyber Threat Intelligence.

Prepare

As cyber threats escalate, your technology architecture, security processes and cultural strategy must evolve to keep pace. Deloitte's cyber prepare solutions can help you put the right defense mechanisms into place, stress test your plans through cyber simulations and implement the behavioural changes necessary to strengthen your cyber security posture.

Related services: Cyber awareness, Cyber governance and cyber security policies

Detect

Massive data proliferation continues to challenge security teams, making it difficult to uncover, identify and respond to potential breaches in a timely manner. Deloitte's detect offerings help bolster your internal resources and deliver access to analytic solutions that make it easier to discover cyber breaches before they cause harm.

Related services: Managed Security Services (MSS); Security Information and Event Management (SIEM).

Respond

When a cyber incident occurs, the response must be immediate, thorough and decisive. Deloitte's cyber response services can provide you with access to the skills, experience and knowledge needed during times of crisis. In addition to establishing the nature of the incident, we work with you to calculate and minimize damages, uncover the root causes of the incident and remediate exposures to prevent future loss.

Related services: Managed Security Services (MSS); Security Intelligence Operations Centre (SIOC).

Managed Security Services (MSS)

Free up in-house resources with outsourced solutions

As cyber threats evolve, it gets harder for internal security teams to detect and address advanced threats around the clock. The resources required to effectively monitor all applications and devices, implement emerging security controls or even analyze security logs can be staggering.

Managed security services relieve that burden by providing you with advanced security event monitoring, analytics, cyber threat management and incident response.

Benefits

- **Predict and prevent security incidents based on past and ongoing events**
- **Improve the effectiveness of your security controls**
- **Reduce compliance and regulatory risk**
- **Gain current and dynamic awareness of the cyber threats endangering your assets, networks and data**
- **Enhance threat detection and response**

Services include the following:

- **Service portfolio management and onboarding:** an effective cyber security program begins with strategic planning. Deloitte professionals have the experience to help you build a SIOC business case, assess your cyber security readiness and discuss the potential impact of cyber threats with your board.
- **Intelligence, Surveillance and Cyber Watch:** to help you keep track of global cyber threats, Deloitte conducts in-depth threat surveillance, threat indicator analysis and cyber chatter analysis and delivers ongoing reports to keep you in-the-know.
- **Security monitoring and advanced analytics:** the Deloitte Cyber Intelligence Centre (CIC) will monitor your systems around-the-clock while leveraging advanced techniques such as predictive analytics and adaptive risk modeling to detect advanced threats.
- **Analysis, investigations, CERT and containment:** to help you prepare for an attack scenario, Deloitte will work with you to run cyber simulations and develop a robust response plan. If an attack does get through, we can also help with response coordination, forensic investigation and root cause analysis.
- **Content development:** by monitoring hundreds of intelligence sources, Deloitte maintains the most current threat content possible, sharing new signature recommendations and new detection scenarios.
- **Executive and operational reporting:** get detailed reports on threat conditions, SIOC process enhancements, configuration enhancements and a range of other metrics that apply to your organization.

Cyber Threat Intelligence

Uncover and address vulnerabilities in your cyber profile

In today's digital landscape, the traditional approach to security no longer works. Firewalls don't consider infection vectors like phishing attacks and SIOCial engineering. Malware and anonymization techniques can circumvent current security controls. Even intrusion detection systems and anti-virus solutions are becoming obsolete.

To manage cyber risk, you need an intelligence-based approach – one that uses knowledge of cyber adversaries and their methods, combined with knowledge of your own security posture, against those adversaries and their methods. Cyber threat intelligence delivers by producing actionable intelligence organizations can use to make informed risk decisions. Its components include the following:

- **Internal and external intelligence gathering**: Deloitte aggregates, maintains and manages a repository of over 300 intelligence sources, including cyber criminal surveillance intelligence.
- **Normalization**: analyzes captured intelligence to identify emerging or active security threats.
- **Enrichment**: provides a comprehensive understanding of the organization's ability to counter cyber threats.
- **Fusion**: strengthens your overall security posture with security control updates, authentication decisions, risk assessment intelligence, technology investment intelligence and assistance with vendor selection and HR decisions.

Benefits

- **Access timely, actionable intelligence to defend against sophisticated cyber attacks**
- **Learn how to apply that intelligence to your environment**
- **Identify and manage internal threat use cases and correlation opportunities**
- **Gain a holistic view into your organization's internal and external threat profile**
- **Benefit from situational awareness across industries, criminal techniques, exploits and vulnerabilities**

Security Intelligence and Operations Centre (SIOC)

Build and operate a world-class cyber SIOC

A Security Intelligence and Operations Centre (SIOC) is an evolution to the conventional SOC (Security Operations Center) that builds and fuses intelligence as the major tenant of the monitoring and threat response capability.

Leveraging decades of SIOC implementation experience, Deloitte can help you overcome these challenges. Our Adaptive Cyber Watch (ACW) SIOC methodology provides you with the tools and accelerators you need to assess, plan and implement a business-centric, high-performance SIOC.

Services include the following:

- **SIOC strategy development**: following a readiness assessment and feasibility analysis, we help you build a SIOC roadmap focused on delivering a return on your investment.
- **SIOC preparation**: assess available vendor solutions, develop a project charter and risk management plan, create a governance structure and adopt appropriate controls.
- **SIOC implementation**: design and stage your SIOC architecture, implement security management protocols and identify the people, processes and technologies that can help you succeed.
- **SIOC optimization**: improve your SIOC processes with cyber SIOC accelerators, a metrics program, escalation procedures and integration with enterprise processes.

Benefits

- **Access timely, actionable intelligence to defend against sophisticated cyber attacks**
- **Learn how to apply that intelligence to your environment**
- **Identify and manage internal threat use cases and correlation opportunities**
- **Gain a holistic view into your organization's internal and external threat profile**
- **Benefit from situational awareness across industries, criminal techniques, exploits and vulnerabilities**

Deloitte Advanced Threat (DAT)

Combat advanced, adaptive and persistent threats

Organizations are increasingly exposed to sophisticated and adaptive cyber threats – one that evade normal detection controls or hide behind seemingly-normal behaviour. Unfortunately, most existing controls focus on threats that cyber criminals have long left behind. Rather than evolving with a polymorphic, rapidly-shifting threat environment, they tend to focus on point-in-time threats and legacy use cases.

Deloitte Advanced Threat (DAT) uses a series of content, processes, threat accelerators, intelligence, workflow and enablers to help you counter the most advanced threats. Powered by ArcSight, the engine is designed to negate the weaknesses of typical monolithic security systems.

Benefits

- **Access cyber threat intelligence from over 300 external and internal intelligence sources**
- **Automatically discover and shut down rogue network devices**
- **Keep pace with evolving threats with an adaptive risk model**
- **Monitor threats and clandestine activity with predictive analytics**
- **Achieve a higher degree of situational awareness**
- **Accelerate investigations with advanced threat queries and reporting**

Security Information and Event Management (SIEM)

Accelerate cyber threat discovery and recovery

Even though most data breaches are persistent and ongoing, organizations frequently fail to detect them. The reasons are varied: some organizations have no security log management strategy, some systems don't work properly and some logs are simply not examined. As a result, organizations lack visibility into external and internal threats, data misappropriation and misuse, virus outbreaks and other high-impact security incidents.

To accelerate cyber threat discovery and recovery, organizations must strengthen their security information and event management (SIEM) systems. With experience deploying all major SIEM tools, and integrating SIEM into existing IT processes, Deloitte can help. Steps include the following:

- **Log collection**: collect data from security devices using a range of methods and protocols.
- **Data normalization and aggregation**: create standard message formats and aggregate the data based on various criteria.
- **Data correlation**: sort data, determine relationships between log events and assign weighted threat values to each event.
- **Event notification**: via email, remedy tickets or other means.
- **Reporting**: provides capabilities to query log events stored in the database and visualize events and trends.

Benefits

- **Reduce the severity and cost of security breaches by accelerating incident response and recovery**
- **Track threats in real time with advanced correlation of meta data**
- **Improve security policy enforcement**
- **Gain the ability to analyze applications and detect anomalous behaviour**
- **Enhance security compliance**
- **Integrate SIEM with your overall security management architecture**
- **Reduce the potential for system disruption from cyber threats**

Advanced Threat Content and End Point Management

Discover your weaknesses

Cyber attackers are always searching for new vulnerabilities. To protect your critical assets, you need to assess and verify your vulnerability exposure, identify which threats are relevant to your organization and take pragmatic action to enhance your security.

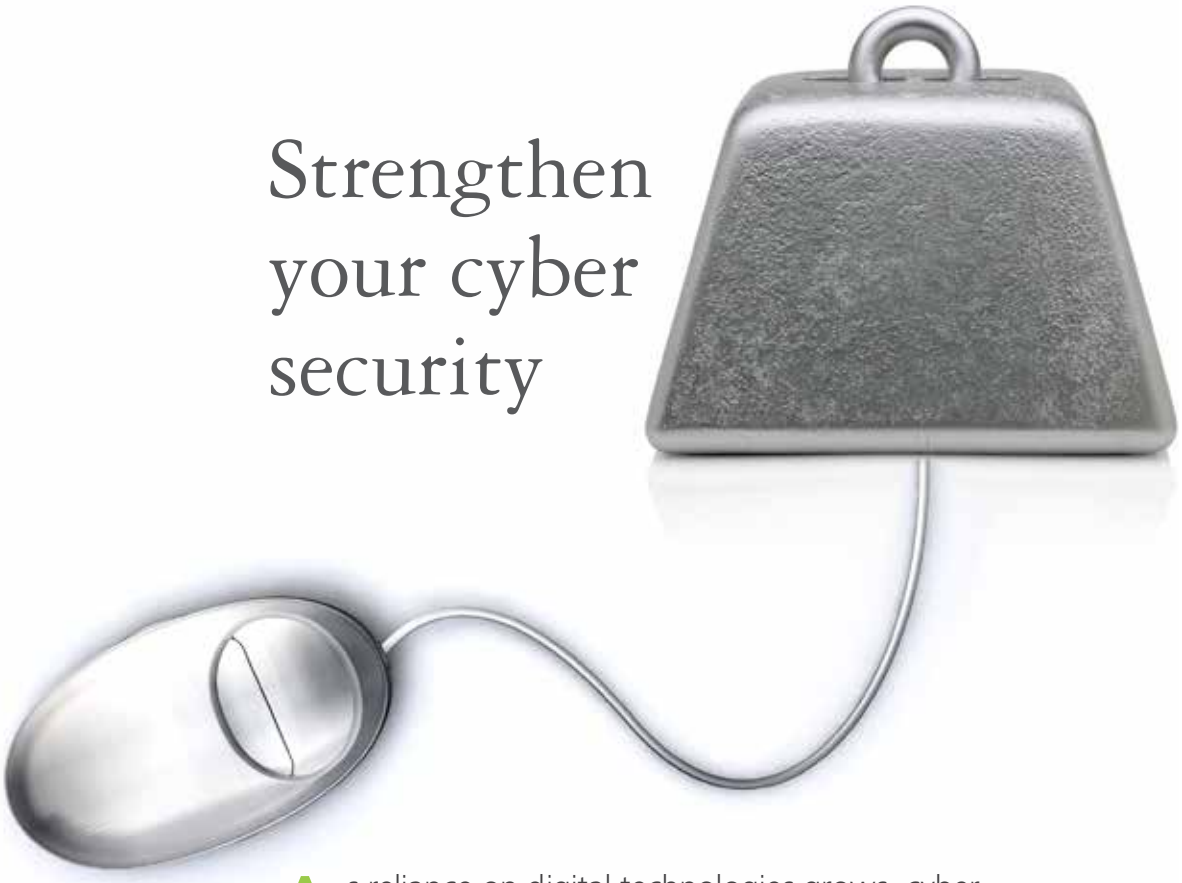
Deloitte's team of vulnerability management professionals can run regular light-tough vulnerability assessments, scanning your entire organization's systems and processes to help identify new and existing weaknesses and map their corresponding impact to your business. Services include the following:

- **Penetration testing**: our penetration testers help with your day-to-day vulnerability management, going as far as hackers would to try and gain access to, or compromise, your systems. With a clear picture of your vulnerabilities and their potential impacts, we can provide recommendations for remedial action to strengthen your cyber defenses.
- **Managed data loss prevention**: to increase the effectiveness of your data loss prevention measures, our team can take over your day-to-day operations, as well as investigating and remediating any incidents discovered.
- **Cyber simulations**: our simulation professionals work with you to test and refine your cyber incident management strategy against realistic scenarios to identify errors, false assumptions and gaps in your plans.
- **Deloitte Fusion**: Deloitte's Cyber Security Fusion Centre provides access to near real-time cyber intelligence to keep you informed about new threats that can affect your industry, infrastructure or deployed technology.

Benefits

- **Enhance your threat detection results with manual testing of your target environment**
- **Understand how hackers work and the damages they can cause to your organization**
- **Protect your business-critical processes and systems from evolving software vulnerabilities**
- **Improve your overall security posture, as well as your incident detection and response capabilities**
- **Identify and address exploitable weaknesses**
- **Leverage international best practices with access to Deloitte's worldwide Security Technology Centres**

Strengthen your cyber security



As reliance on digital technologies grows, cyber adversaries have become extremely inventive in their attacks. Organizations that continue to rely on outmoded security measures leave themselves increasingly vulnerable – exposing themselves, their stakeholders and the economy at large to the potential for severe damage.

To counter these threats, it's time for organizations to refine their cyber security programs. Beyond enhancing regulatory compliance, an effective cyber security program can help organizations disrupt attacks as they happen, reduce the timeframe and costs of recovery, and contain future threats.

No matter where you are in the cyber security lifecycle, Deloitte can help you strengthen your security stance. With a flexible, pragmatic and independent approach to cyber security, we can work with you – from the network to the boardroom – to address the constantly changing threat landscape.

Cyber security maturity model

For more information on cyber threat, please contact:

National contacts

Nick Galletto
Partner
Enterprise Risk Services
416-601-6734
ngalletto@deloitte.ca

Mark Fernandes
Partner
Enterprise Risk Services
416-601-6473
markfernandes@deloitte.ca

Regional contacts

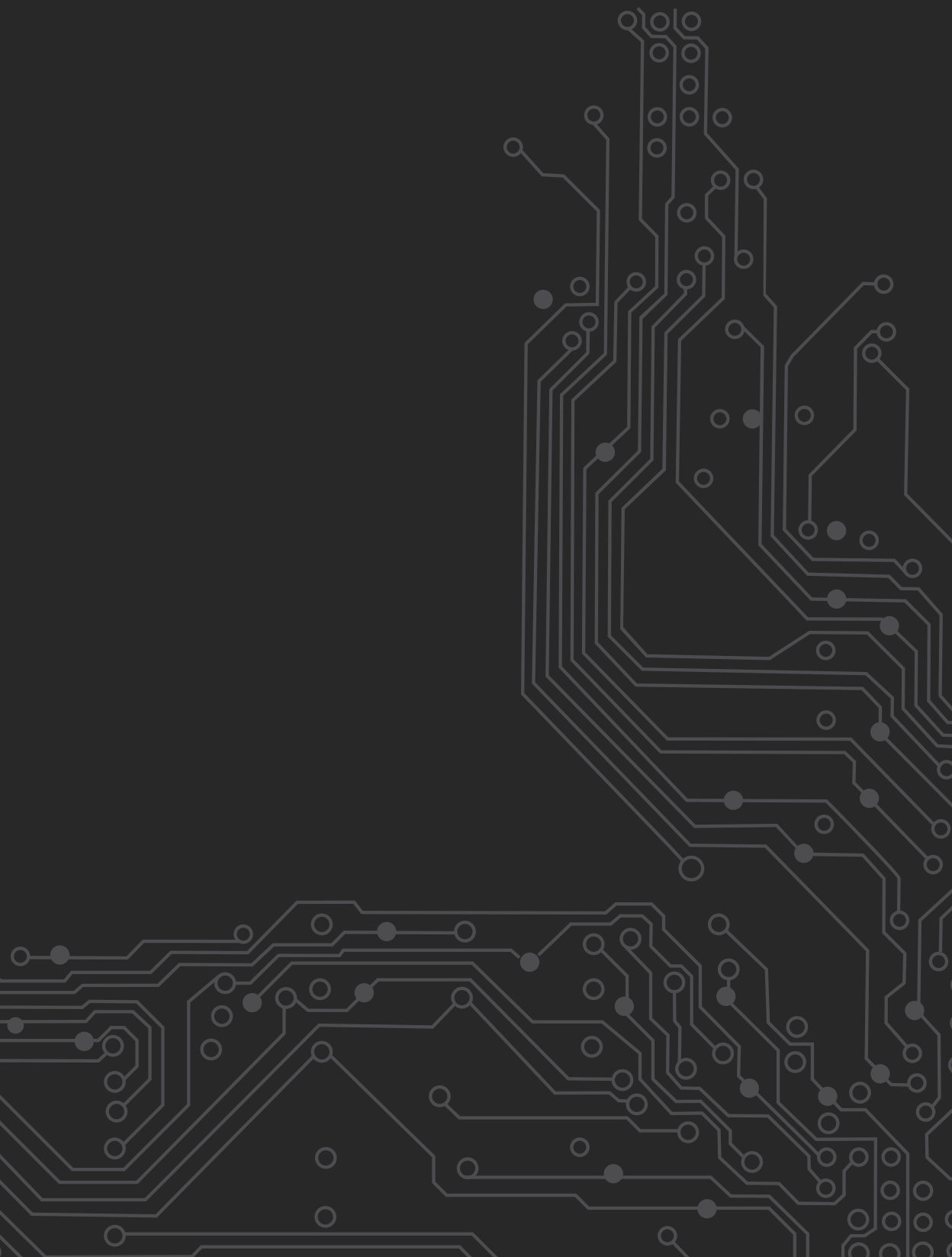
Amir Belkhelladi
Partner
Enterprise Risk Services
514-393-7035
abelkhelladi@deloitte.ca

Alain Rocan
Partner
Enterprise Risk Services
613-751-5386
arocan@deloitte.ca

Justin Fong
Partner
Enterprise Risk Services
403-503-1464
jfong@deloitte.ca

Albert Yap
Partner
Enterprise Risk Services
604-640-3279
ayap@deloitte.ca

Dina Kamal
Senior Manager
Enterprise Risk Services
416-775-7414
dkamal@deloitte.ca



Endnotes

1 International Cyber Security Protection Alliance, May 2013.
"Study of the Impact of Cyber Crime on Businesses in Canada."
Accessible at https://www.icspa.org/fileadmin/user_upload/Downloads/ICSPA_Canada_Cyber_Crime_Study_May_2013.pdf.

2 Source: Kennedy Consulting Research & Advisory; Cyber Security Consulting 2013;
Kennedy Consulting Research & Advisory estimates

www.deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 13-3694