Cyber724.com

Products and Services

To Our Valued Clients,

For many months, indeed for many years, cyber criminals have been working brazenly around the world, unimpeded by laws, borders or physical barriers; taking confidential information at will, deleting files, participating in extortion schemes and engaging in identify theft.

Vast amounts of business and personal wealth have been lost. Organizations have closed, cities held ransom, government secrets exposed, operating rooms shut down, and public transportation systems have been compromised.

The anonymity that cyberspace provides criminals has dramatically accelerated this type of crime. Cyber-crime rings are well funded and well organized. Many cyber criminals are even state sponsored.

Cyber criminals are technically advanced. They adeptly seek out every possible operating system and security vulnerability and exploit these to their benefit. They continuously enhance the sophistication of their attacks, they innovate and adapt and as a result, they become more effective at their dark art.

Unfortunately, the time has come for individuals and businesses to stop assuming the best of people. The time has come to set up strong defenses against these well-trained criminal elements that are smart, armed with deceptive technologies and are driven by malicious intent.

Cyber724 is our response to the market's demand for answers to this unrelenting threat. The products and services described in this pamphlet are intended to help our clients understand the risks they are facing, and to know what steps they can and should be taking to protect themselves.

Through our work with legal experts, we can help our clients prepare, document and enact, industry tailored cyber security policies that could provide important evidence to legal authorities and regulators, should the need ever arise.

If you have any questions, or you would like to arrange for a call or visit, I can be reached at any time.

Sincerely,

Brian Everest
CTO
Cyber724
brian.everest@cyber724.com

1-888-435-7320 x 724

CyberRisk – Challenges and Responses

"The loss of industrial information and intellectual property through cyber espionage ***constitutes the greatest transfer of wealth in history***."

- General Keith Alexander, Former NSA Director and first Commander of United States Cyber Command

Cyber security is an increasingly vital business function that is significant to every aspect of corporate health. An appropriate and proactive cyber security function affects:

- Investor confidence
- Brand reputation
- Product and service integrity
- Customer confidence
- Corporate culture and resulting staff behaviour
- Operations reliability and efficiency
- Regulatory compliance

Cyber-attacks are evolving rapidly, becoming more frequent, and are increasingly dangerous to on-going business operations. The risk of cyber threats is not new, but the levels of sophistication, the speed of attacks, and the severity of damage that can be inflicted are alarmingly new.

With stakes so high, organizations must evaluate their risk tolerance and how they will respond to cyber security threats. Many senior level executives are unaware of their responsibilities to manage compliance, and to affirm for customers, stakeholders and employees, that appropriate safeguards are in place.

In response to this urgent need, Starport Managed Services has come to market with a suite of services that will help organizations of all sizes build a defence, and protect themselves from data loss, business disruption and possible extortion.

Starport delivers its cyber security services through its team of security professionals located at Starport's Security Operations Centre (SOC). The security operations center staff is comprised of IT security professionals who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Our Cyber Security products and services are described in the following pages.

CyberAsessment

We conduct a deep analysis and review of your current IT defences and procedures, and provide you with a detailed review of your organization's ability to protect its information assets and to defend itself against cyber threats.

A CyberAsessment looks beyond pure technical readiness for cyber threats. We take a rounded view of people, processes and technology. This enables you to understand areas of vulnerability, identify and prioritize areas for remediation and demonstrate compliance, turning information risk to business advantage.

Upon completion of a CyberAssessment, you'll receive a report that provides a comprehensive view of your organization's level of cyber maturity. We will look at:

- The current tools systems and processes to protect your organization against cyber attacks
- Vulnerabilities that need immediate attention
- Your organization's IT culture, providing suggestions for improving staff attitudes towards security
- Your organization's preparedness for the evolving cyber security landscape
- Your existing cyber security strategy (if it exists) and areas to be updated, changed or improved
- The extent to which your cybersecurity framework complies with legally required privacy and security measures, to identify areas of non-compliance.

CyberWatch

After the Cyber Security environment has been configured, the analytics and data produced by our security appliances will be monitored by Cyber724's SOC. The SOC is staffed by IT security professionals whose goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and established processes.

Staff at our SOC monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise.

Cyber724 will provide periodic updates on cybersecurity legal requirements, as these evolve through changes in law and regulatory guidance.

CyberCheck

Our Penetration Testing methodology seeks to uncover vulnerabilities residing in IT systems, human beings, applications or network components and attempts to exploit them to obtain access to sensitive information.

Our security consultants are skilled at identifying weaknesses that overlook. Our staff are continuously updating their skills, learning new ways to evade controls in modern networks. We take the time to understand each component and its role in the overall system and custom tailor our approach to each environment we assess.

A penetration test should ideally be conducted by every organization on an annual basis. It is very thorough, usually taking 2-3 days to complete over an elapsed period of one week. At the conclusion of a penetration test, any areas of defence that need to be reinforced will be identified and reported to you.

Cyber724.com

CyberLearn

Your people are at the front line in the cyber-war. The most pervasive threats, including phishing and ransomware, target users to breach your security defences.

Statistics and studies around the Internet paint a grim picture:

- 30% of phishing emails get opened
- 90% of the phishing emails contained ransomware
- 33% of companies have been the victim of CEO fraud (spear phishing or BEC attacks)
- The number of data breaches increased by 40% in 2016 to more than 4.2 billion records
- 123456 is still the most popular password.
- When end users know what to look for, the risk of a breach reduces dramatically.

The CyberLearn on-line portal provides users with Security Awareness Training that breaks down key security concepts and threats into plain English and real-world stories, so anyone can understand and know how to manage cyber-threats.

With its modular design, Starport's CyberLearn presents each topic on a self-contained basis. New modules are added as new threats and subject matter areas emerge. The current topics available in CyberLearn include;

- Data Protection
- Passwords
- Email and Phishing
- Social Engineering
- Malware and Ransomware

Features

- Key security elements, de-geeked and made simple for everyone to understand
- Short, focused modules on key security areas including data security, passwords, phishing and other email scams, ransomware and social engineering
- Real-world stories to show applications of key concepts
- Access to regular live security webinars and other training materials
- Testing to ensure comprehension

Training Formats

- Online training through our portal
- Live in-person or webinar training

About Starport Managed Services

Starport is a managed IT services company that serves a client base of over 100 companies and has been in business for over 14 years. Our staff of more than 40 manage 2 data centres; one co-located and one wholly owned. We also have a wholly owned, fully staffed Service Desk located in Summerside PEI.

Starport delivers best in class IT design, implementation and continuous network monitoring to mid-sized organizations. Clients come from a variety of industries including investment banking, pharmaceutical, transportation, food & beverage, technology, consumer packaged goods, manufacturing, commercial real estate and not-for-profit. We are proud of the work we do, and we believe we add a strategic edge to every client we work for.

Starport and its wholly owned information security subsidiary, Cyber724, assist mid-sized enterprises who value the importance that IT plays in the smooth functioning of their operation. When well designed and deployed, IT infrastructure can and should provide significant strategic edge to Canadian businesses. Supporting and protecting Canadian businesses is our reason for being.

Cyber724.com

Your Organization is an Attractive Target to Hackers.

Never think:

"It Won't Happen to Us"

info@cyber724.com

(416) 479-8241 x724

1-888-435-7320 x 724

Because a cyber defense strategy based on hope, is just wishful thinking