starport MANAGED SERVICES

Cyber724 Protection

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 any type of traditional 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 has been lost. Organizations have closed, government secrets exposed, operating rooms shut down, public transportation systems have been compromised.

Cyber-crime rings are often well funded and well organized. There is compelling evidence that many cyber criminals are even state sponsored.

Cyber criminals are technically very advanced. They adeptly seek out every possible operating system and security vulnerability and exploit them to their benefit. They continuously enhance the sophistication of their attacks, they innovate and they 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 this well-trained criminal element that is smart, that is armed with deceptive technologies and which is relentlessly driven by sinister intent.

As CTO and co-founder of Starport Managed Services, I'm taking the threats posed by cyber criminals very seriously. That's why I've created a new cyber security unit called, Cyber724 Security Solutions.

Cyber724 is Starport's 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.

You'll also see that we have established a relationship with Fasken, a law firm in the area of cyber policy. Through our work with Fasken, we can help our clients prepare, document and enact strong, industry tailored cyber security policies that could provide important evidence to legal authorities and regulators should the need ever arise.

I trust you'll find this document to be of assistance as you set out to build your defences. 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
Starport Managed Services
brian.everest@starport.ca 1-888-435-7320 x 724

CyberRisk – Challenges and Responses

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Robert S. Mueller, III, Past Director FBI

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

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

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 understand their cyber security 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 introduced 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 sections following.

CyberAudit

Starport's CyberAudit is a service in which 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 CyberAudit looks beyond pure technical readiness for cyber threats by taking a rounded view of people, processes and technology, to enable 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 CyberAudit, 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 attack
- ✓ Vulnerabilities that need immediate attention
- ✓ Your organization's IT security culture and provide 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.

CyberConfig

After the completion of a CyberAudit, the next step many organizations will take is to implement some or all of the recommended changes to their processes and IT environment.

Some of the typical implementation outcomes of Starport's CyberConfig may include:

- ✓ Installing new hardware
- ✓ Conducting upgrades to operating systems
- ✓ Applying patches to servers and workstations
- ✓ Reconfiguring firewalls
- ✓ Adding new layers of backup
- ✓ Developing, implementing and testing a disaster recovery plan
- ✓ Geo-blocking and perimeter protection
- ✓ Configuring, installing and implementing a cyber security specific 7x24 monitoring appliance.
- ✓ Encryption of data on notebooks (e.g. Bitlocker)

The 7x24 cyber monitoring appliance will generate reports on a periodic or "on demand" basis. It will be configured to meet established specifications to ensure continuous, effective monitoring.

At the conclusion of the CyberConfig stage, your IT environment will be updated, secured and ready for continuous monitoring and reporting.

CyberWatch

After the Cyber Security environment has been configured, the analytics and data produced by Starport's Cyber Security appliance will be monitored by Starport's SOC. Starport's 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.

Provide periodic updates as to 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, applications or network components and attempts to exploit them to obtain access to sensitive information.

Our security consultants are skilled at identifying weaknesses that others (except cyber thieves) overlook. Our staff are continuously updating their skills, learning new ways to evade controls in modern networks. We take the time to understand each of the in-scope components and their 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 a 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.

CyberPolicies

You might have top-of-line Cyber security, but if you don't have policies documenting your practices, you'll be significantly disadvantaged. Your Cyber security policies form the core of your Cyber security program, as they are the basis for employee training and the baseline for updates as Cyber security standards evolve, and – perhaps most importantly – provide evidence to regulators that you have a documented Cyber security program in place should the need ever arise.

As part of its suite of Cyber Security services, Fasken and Starport will document your Cyber security program, and will update same as your Cyber security program evolves.

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.

Starport's 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
- ✓ Key Elements of Privacy and Security Legal Compliance
- ✓ Cyberlaw Update (Annual)

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

- ✓ Use of our online training portal
- ✓ Live, in-person or online training

About Starport Managed Services

Starport is a Toronto based managed IT services provider. It delivers best in class IT design, implementation and continuous network monitoring to mid-sized organizations primarily headquartered in the Toronto area. Clients come from a variety of industries including investment banking, manufacturing and commercial real estate to name a few.

About Fasken

Fasken, formerly Fasken Martineau DuMoulin, is an international business law firm with more than 700 lawyers and offices in Vancouver, Surrey, Calgary, Toronto, Ottawa, Montréal, Québec City, Beijing, London and Johannesburg. Fasken is a recognized leader in technology law. Respected peer review publications such as Chambers, Lexpert, Who's Who Legal, Best Lawyers, Practical Law Company and others frequently recognize our team for its skill and contributions to organizations such as the International Technology Law Association (ITechLaw), the Canadian IT Law Association (IT.Can) and the International Federation of Computer Law Associations (IFCLA).

FASKEN

Your Organization is an Attractive Target to Cyber Thieves

Don’t ever Say

“It Won’t Happen to Us”

Email us today at: cyber724@starport.ca
or call
1-888-435-7320 x 724

because a cyber defense strategy based on hope is just wishful thinking