Cyber Security Good Governance

A Management Primer on Cyber Security Responsibilities

- How are cyber threats evolving?
- What do you need to get ahead of them?
- How do you build a robust security regime?
- What options do you have?

Cyber Security Management Imperatives

Small businesses were generally ignored by cyber security criminals. Not anymore. We're suddenly prime targets for the bad guys and we're all struggling to keep up. This eBook is a primer for conversations between C-suites, boards of directors and investors. It's also a "how to guide" for driving cyber security changes in the face of budget challenges and expertise shortages.

Robert Bracey
President and CEO
Quartet Service Inc.

The Perfect Storm?

This may be the golden age for SMB (Small/ Medium Businesses) cyber crime as criminals target this unsuspecting and underprepared sector. Cyber crime skill requirement is decreasing as cyber crime tool power is increasing. The number of cyber criminals and the variety of attack vectors are all on the rise. Expectations and preparations must shift from "if" to "when". It is worse than you think.

Business Case Ambiguity

Cyber crime is a global growth industry estimated at $7 trillion. $7 trillion! This innovative marketplace includes rental hacks, time shares, pay-per-intrusion schemes and others. Cyber criminal collaboration is driven by clear business cases and proven outcomes. Unfortunately, SMB cyber security business cases are ambiguous. Return on investment cannot be measured in the traditional sense. The statistics showing the massive impact of cyber crime on SMBs are clear, but it still takes an enormous amount of vision to properly protect your business.

Collaboration is Mandatory

The cyber crime world is too vast, changing too fast and requires such specialized training, that it's impossible for a lone SMB to keep up. Collaboration between security tool suppliers, service providers and SMB staff is mandatory. But, collaboration is not native to traditional IT culture. Good cyber security management is a behavioral challenge as much as anything else. The biggest cyber security challenge for many SMBs is change management.

This book provides insights for business leaders to drive organizational change. It contends that modern cyber security programs require collaboration between tool developers, service suppliers, internal staff and management.

Modern cyber security programs address this challenge in an affordable and comprehensive way.

Regards,

Robert Bracey

If It Can Happen, It Will Happen

The new #1 cybercrime target is small to medium-sized businesses—over 60% have experienced a cyberattack in the past 12 months.[1] You simply don't hear about them because they aren't sensational and aren't made public.

WAIT, THERE'S GOOD NEWS.

The cyber landscape is transforming. And since we know how it's transforming, you can get ahead of the curve and mitigate the damage. Better yet, you can become a tougher target so that attackers move on to lower-hanging fruit.

At Quartet, our business is constantly under attack—we know this because as an IT service company we must monitor and log all attacks. There are hundreds of these each week and they are getting more sophisticated all the time. Want to guess what's happening to your business?

It's not about when you'll get attacked.

YOU'RE ALREADY BEING ATTACKED.

This short eBook will help you understand what it takes to protect your business against cyber threats in this new era...and teach you what you need to do to make that happen.

[1] 2017 State of Cyber Security in Small &Medium-Sized Businesses (SMB), publication, Ponemon Institure LLC, September 2017, accessed September 2018, http://www.veille.ma/IMG/pdf/2017_state_of_cybersecurity_in_small_medium-sized_businesses.pdf.

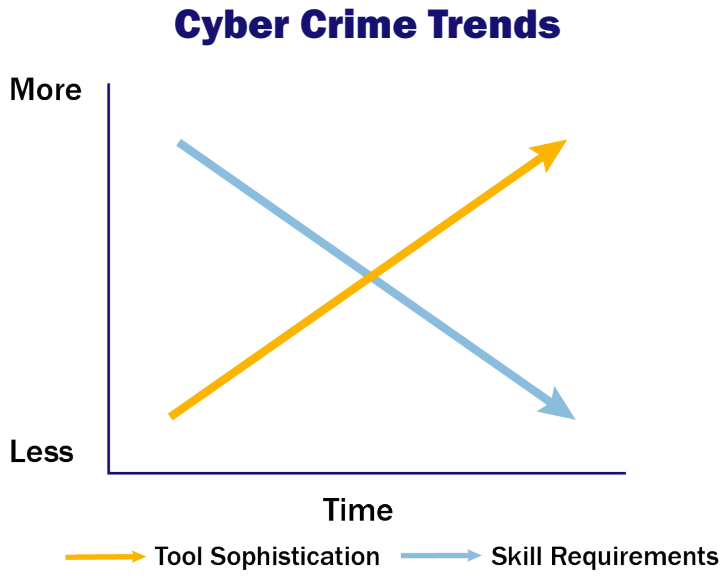
Target: SMBs

Cybercrime used to be difficult. Hackers had to build their own tools and vertically integrate their operations, from gathering information on targets to spoofing websites, to collecting funds the old fashioned way.

Now hackers use robust tools that are readily available on the Dark Web, the part of the Internet that can't be found using regular browsers and Google searches. Only 4% of the Internet is readily accessible; an incredible 96% is untraceable and accessible via special browsers.

These days, you don't need to be a techie to carry out cybercrime exploits. Dark Web actors sell lists of email addresses and credit card numbers as well as complete personal profiles. They also provide the means to exploit them, such as plug-and-play crimeware, exploit kits and ransomware. Pay for what you need in Bitcoin, and you have the means of executing cybercrime.

Cyber exploits are not difficult to execute. It just takes one click on a nefarious email: a simple phishing campaign locked down the computer systems in the Town of Wasaga Beach, Ontario in early 2018, incurring $35,000 in ransom, $50,000+ in consulting fees and hundreds of thousands in lost productivity.[2]



As time passes, tool sophistication increases and the skills required to hack SMBs decrease.

[2] Dawn Calleja and Steve Brearton, "How to Hack-Proof Your Employees," The Globe and Mail, September 28, 2018, accessed September 2018, https://www.theglobeandmail.com/business/rob-magazine/article-how-to-hack-proof-your-employees/.

Why SMBs?

Faced with ever more sophisticated enterprise defenses, cybercriminals are targeting the low-hanging fruit: SMBs. The size of the prize may not be as big, but getting it is far easier. Not only are there more hackers out there, but the cost of launching a cyberattack has decreased dramatically.

Simply put, large enterprises have huge resources; smaller companies have few. Canadian banks are known for having world class security, and no wonder: the stakes are sky high, so they allocate the resources. Banks have well-developed, well-funded cyber security departments and a full complement of security consultants. They each spend millions of dollars each year on cyber defense.

The spend is justified because—and this is important—the precautions that the Big Five take are commensurate with the potential consequences of a breach.

31%

31% of small businesses take active measures to guard themselves[3]

22%

22% of small businesses are willing to improve their security measures from last year[4]

[3]Wes Spencer and Eric Foster, "Finding Your Inner MSSP: The Easiest Way to Add Cybersecurity to Your Mix" (IT Nation Connect, Orlando, Florida, November 2018).
[4] ibid

Your Biggest Attack Vector: Employees

A robust firewall and endpoint security used to be the mainstays of corporate cybersecurity. They are still necessary, but there are dozens of ways to penetrate your organization other than frontal attacks. The common denominator among these is they target your employees, specifically our core human weakness: between 80% and 90% of data breaches are caused by errors in judgment[5]. Your employees aren't stupid. But they are human.

41%

41% of small businesses are unaware of the risks accrued with human error[6]

[5] Dawn Calleja and Steve Brearton, "How to Hack-Proof Your Employees," The Globe and Mail, September 28, 2018, accessed September 2018, https://www.theglobeandmail.com/business/rob-magazine/article-how-to-hack-proof-your-employees/.
[6] Wes Spencer and Eric Foster, "Finding Your Inner MSSP: The Easiest Way to Add Cybersecurity to Your Mix" (IT Nation Connect, Florida, Orlando, November 2018).

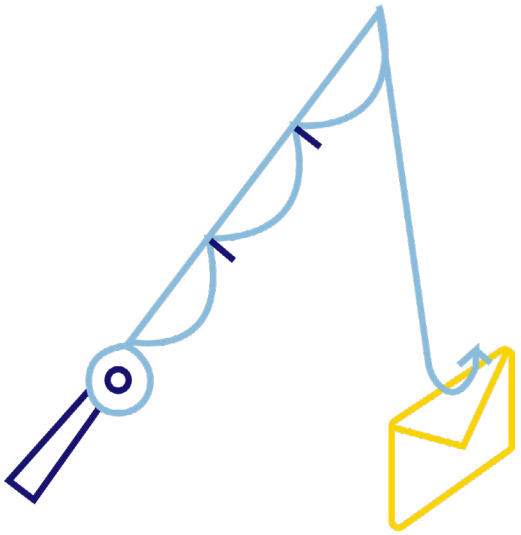
Don't Be an Easy Target

Three vulnerabilities worth highlighting are phishing, ransomware and mobile devices.

Spear Phishing

Phishing is when you are encouraged, typically within a fraudulent email, to click on a link or to open an attachment that takes you to an infected website or downloads malware onto your computer. We all get them: a message supposedly from a beautiful Russian, or your bank. Such emails range from laughably amateur to chillingly convincing. According to Verizon, phishing represents 98% of social incidents and 93% of breaches. On average, 4% of the targets in any given phishing campaign will take the bait.[7]

Spear phishing is a more precise version of phishing: it targets a specific company or even a specific employee. Spear phishing is not uncommon—it has happened right here at Quartet. When our President & CEO Rob Bracey travelled for work, senior staff started getting spear phished. They received emails, supposedly from Rob, asking them to wire sums of money overseas. We identified several possible attack vectors and upgraded the security on all of them, which put an end to it. Our staff didn't fall for any of the ruses, but spear phishing is prevalent because it works so well.



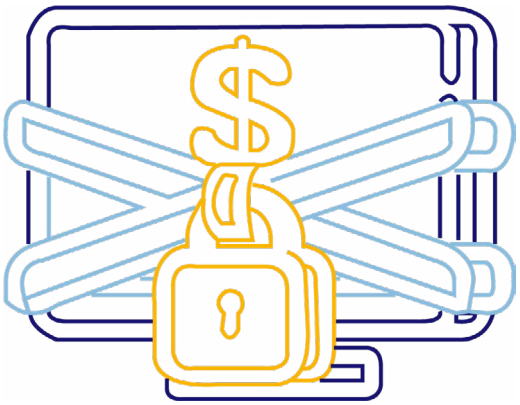
[7]2018 Data Breach Investigations Report, report, Verizon, February 2018, accessed September 2018, https://enterprise.verizon.com/resources/reports/dbir/.

Don't Be an Easy Target

Ransomware

Ransomware is the top category of malicious software, accounting for 39% of identified malware.[8] It freezes computers, accounts and software until a ransom is paid, typically in bitcoin. Ransomware is overwhelmingly installed during successful phishing attacks and exploits a software vulnerability. SMBs in Canada and the U.S. have the highest recovery cost, at U.S. $149,000 on average, up 21% over 2018.[9] A new trend in ransomware is to punch a hole in corporate defenses, then close the door and auction off back door access to the highest bidder. Rather than seeing the whole ransom process through to its conclusion, which can take days or weeks, ransomware experts move on and exploit the same weakness in other organizations.

In 2018, WannaCry ransomware infected close to a quarter million computers around the world in a single day, demanding U.S. $300 in bitcoin to unfreeze infected computers.[10] It took advantage of an unpatched software vulnerability in an older Windows operating system.



Mobile Devices

In the wrong hands, lost smart phones are a real problem for businesses because the applications on these small computers provide an easy backdoor into the corporate environment.

Most lock screen passcodes are easily cracked, so unless you have the ability to remotely freeze or wipe a lost or stolen phone, it's a big worry. Poor password policies combined with more mobile-targeted attacks and poor or non-existent mobile device management (MDM) is a recipe for disaster.

[8] ibid

[9] On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives, report, Kaspersky Lab, 2018, accessed September 2018, https://go.kaspersky.com/rs/802-IJN-240/images/2205_kaspersky_ IT Security economy Report_final_2305.compressed_NA.PDF.

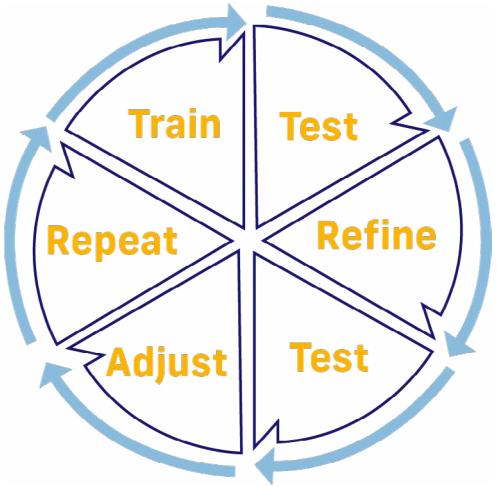
[10] Dawn Calleja and Steve Brearton, "How to Hack-Proof Your Employees," The Globe and Mail, September 28, 2018, accessed September 2018, https://www.theglobeandmail.com/business/rob-magazine/article-how-to-hack-proof-your-employees/.

Don’t Be an Easy Target

Any way you slice it, your employees are almost always your biggest security weakness. The solution is to shape employee behaviour with training, but also to test the results of that training, and to retrain pretty much constantly. That said, firewalls, endpoint protection and employee training are only part of the solution.

Thanks to growing reliance on IT, the day-to-day operations involved in cyber security maintenance have become fundamental to good business management. Virtually all businesses have to embrace technology in order to remain competitive, which increases their exposure to cyber threats.

Employee Behaviour Training



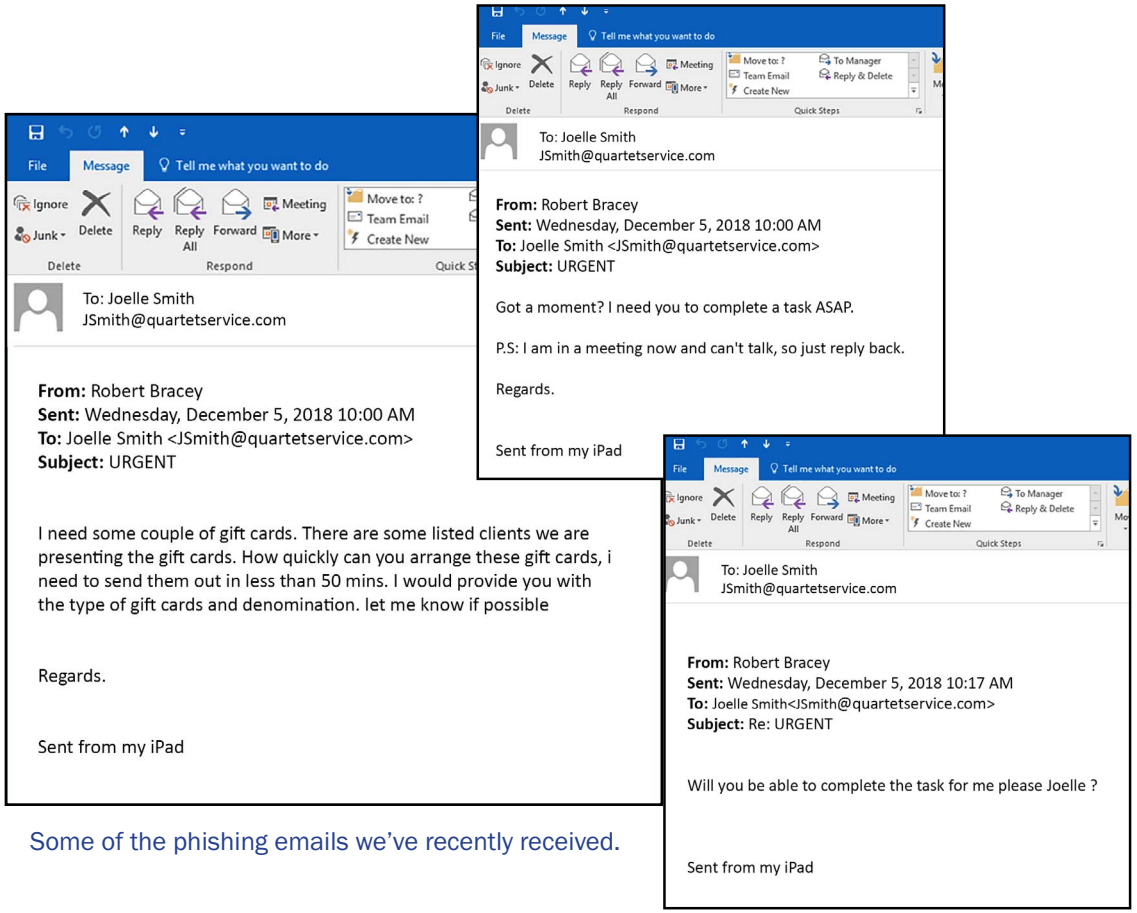
Train your employees, test and refine the training, test and adjust the training as the threat landscape evolves, repeat.

Your Security Ops

True cybersecurity is a mindset: it's not about setting up a perimeter defense to protect servers; it's about safeguarding your entire organization from cyber risks of all kinds. When you adopt that mindset, it becomes less about the employees, or the tools, and more about your overall cyber strategy and cybersecurity operations.

THE CYBER ARMS RACE

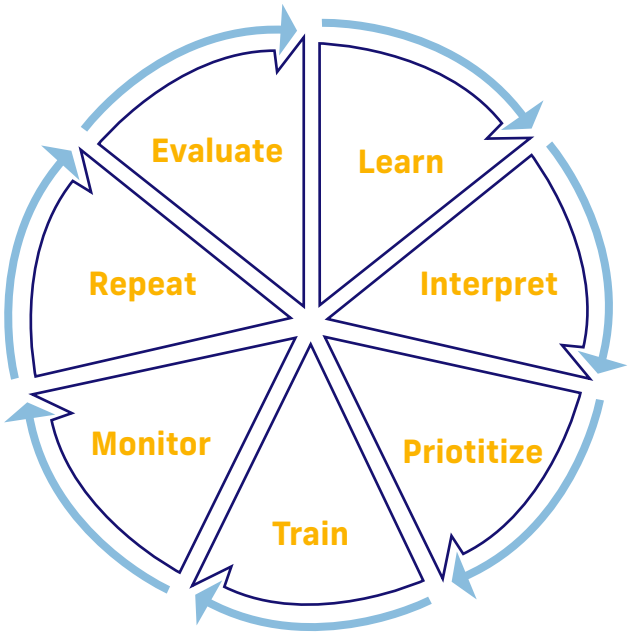
The right tools are an indispensable part of security operations. Today's tools are awesome. They are also changing all the time. You still need endpoint security, but you also need artificial intelligence (AI), heuristic behaviour monitoring and machine learning. Very broadly speaking, this new generation of tools finds trends in billions of data points and identifies nefarious activity before it does serious damage.



Some of the phishing emails we've recently received.

Your Security Ops

The right tools may be critical, but simply having them is missing the point. You have to pick the right tools, learn how to use them properly, and then parse the data. There are some fantastic tools out there, and they are multifaceted. Most are easy to operate at a basic level but quite difficult to master. And most of them give you mountains of data. Confronted with data overload, most people do nothing. But you need to prioritize actions based on what your 15 tools are telling you. Unfortunately, there are no shortcuts—and yet you have to do it all the time.



Evaluate and choose the tools, learn to use the tools efficiently, interpret the data, prioritize & carry out actions, train your staff, monitor staff use of tools, repeat.

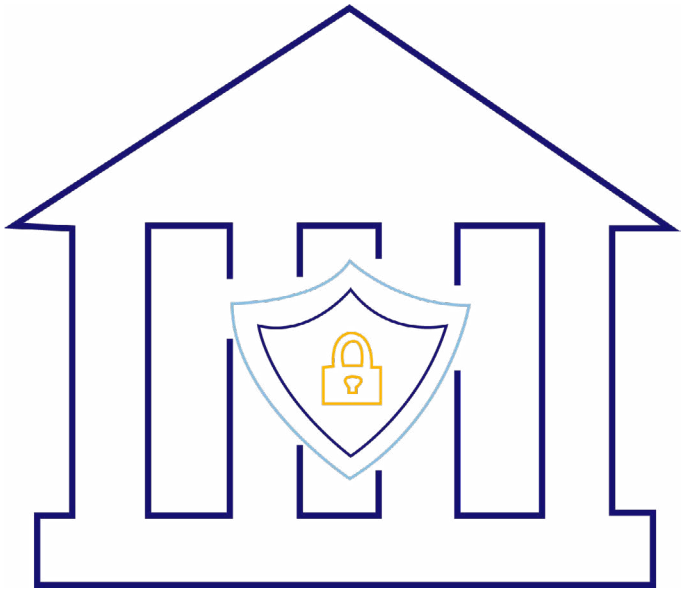
Your Security Ops

At Quartet, we constantly evaluate tools and adopt several new ones per year. For example, we adopted 25 new security tools in 2018. We sandbox each tool implementation, then deploy it internally, and then to customers. We train our employees on the effective use of each new tool. Since the cyber world is essentially a fast arms race, we go through the same multi-step process month after month: evaluate tools, adopt tools, master the tools, train our people, and prioritize actions.

In addition to spending time selecting, learning and training on new tools, the upgrade path also involves constant synchronizing of systems. As soon as you update one component of your IT infrastructure, some other part inevitably stops working and needs fixing. Think about that for a minute. Where does the buck stop?

If you're maintaining IT security infrastructure, when you upgrade something, something else is liable to break. No one is accountable but you. You can't hold the tool vendors to account, nor your CRM, ERP or other system vendors. Each points a finger in the other direction. What this boils down to is that the most difficult part of security is the actual operations. It's tough to keep up: with the tools, with the learning, the training, and the ongoing work.

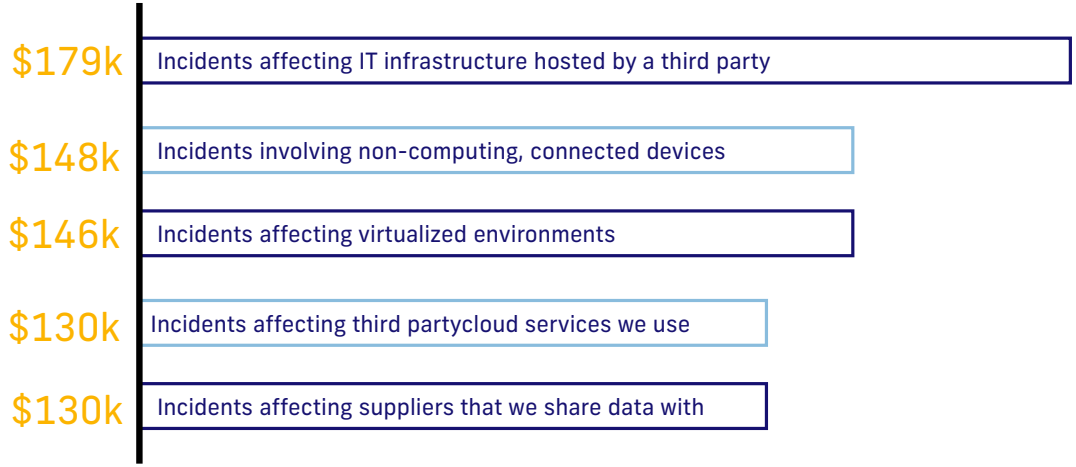
One thing you can count on, though: a cybersecurity event is going to happen.



From ‘If’ to ‘When’

If your organization hasn’t experienced a security breach yet, count yourself lucky, or you might just not know it yet. Our best advice is to be humble: realize that it’s no longer a question of ‘if’ you have a breach, but ‘when’. It’s getting dark out there.

Average Cost of Attacks (USD)[11]



QUANTIFY YOUR RISK EXPOSURE?

How many hours or days can your business survive if it grinds to a halt? How much will your reputation suffer? Your fallback plan for rapid recovery in the event of a breach will depend on its impact on your business. While spending millions might make sense for the banks, it almost certainly won’t work for you.

Average SMB security budgets have grown by 18% from the year previous to U.S. $246,000 in 2018. Very small businesses spent an average of U.S. $3,900 in 2018, an increase of 38% over the year previous.[12]

But averages won’t tell you much—your investment needs to be commensurate with the risk you run. If your business is connected to the Internet and relies on data to keep functioning, whether your operations rely on data or information is what you sell, think about the numbers above.

[11] On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives, report, Kaspersky Lab, 2018, accessed September 2018, https://go.kaspersky.com/rs/802-IJN-240/images/2205_kaspersky_%20IT%20Security%20economy%20Report_final_2305.compressed_NA.PDF
[12] ibid

Preventing Attacks

The path to resilience is clear. Follow these steps to harden your business to cyber attacks and get attackers to move on to an easier target.

Step 1: Back Up Data

You can back up to tape, or move your data in an encrypted fashion into secure cloud storage. Cloud keeps getting cheaper, so it's a viable, redundant alternative to tape. Assuming that you already back up your data, do you test your backups? To make sure that backups are going to work in the event of a disaster, you need to restore your data on a regular basis. Every three or six months could be sufficient, but if you measure acceptable downtime in hours and not days, you will need to restore on a weekly or bi-weekly basis.

Step 2: Implement Security Policies

Implement an IT security policy that's clear and easy to understand. It should include how to use, transfer and store corporate data, protocols for treating email requests (for example to wire funds or send sensitive information, etc.), how to keep smartphones safe and what to do when a security breach is suspected. Spell out clearly what employees should do and also what they shouldn't. Test and update your policies yearly. You must fight security policy entropy. This is a company-wide discipline, not just an IT department responsibility.

Step 3: Get the Tools

Correctly using the right tools is a big part of staying safe. Add to your firewalls and endpoint software with cyber defence tools that leverage AI and machine learning to monitor your environment. Include mobile device management (MDM) if your workers are mobile. Once you have found the right tools, learn to use them to make prioritized decisions and change security posture as required.

Step 4: Train Employees

This step circles back to Step 2. Train employees on IT security according to the policies you have developed. This should include the correct use of programs and tools, but also best practices in their day-to-day interaction with the digital world: what constitutes a phishing email, what to do if phishing is suspected, workstation password-protection parameters, acceptable use of flash drives, and more. Do the training, repeat the training, and test the training. One of the testing techniques that we use at Quartet is an ongoing phishing program. We build phishing emails and try to get customer employees to click. We think of this as inoculating with skepticism. It's something you have to do on a regular basis, or else people let their guard down.

TRAIN FOR INSURANCE

Training is not just a security requirement. It is a cyber insurance requirement and for many industries, a regulatory obligation. Cyber liability insurance payouts are often predicated on adequate employee security training and monitoring. If your employee testing training

Preventing Attacks

on adequate employee security training and monitoring. If your employee testing training monitoring program is good, some insurers will give you a discount.

TRAIN FOR COMPLIANCE

Your cyber security compliance obligations change regularly and have industry specificity. The Personal Information Protection and Electronic Documents Act (PIPEDA) come into effect. For example, on November 1st 2018, Canadian organizations subject to PIPEDA are now required to report to the Privacy Commission all personal information security breaches that pose a real risk of significant harm to individuals. You must notify affected individuals about those breaches, and keep records of all breaches—whether they require reporting or not. In a lawsuit, breach records are the first thing that the defense team is going to ask for. If your people don't have the training and the protocols in place, how can you be sure that you will conform with updated PIPEDA requirements?

You must be able to prove your due diligence and should be able to provide security logs if required.

Step 5: Business Resiliency Planning and Disaster Recovery Planning

CIOs of even the most well-protected organizations will tell you that a cyber event is inevitable. That's why they have cyber response policies and action plans. Think of how you do business—IT and communications mechanisms like email, telephone and information management, but also your physical infrastructure and the suppliers that you rely on to get business done. Do you have any single points of failure anywhere along your supply chain? Critical components that are single-sourced?

Business Resiliency Planning (BRP) identifies ways to carry on with business in the event of a supplier failure, a cyberattack, or an Act of God. Disaster Recovery Planning (DRP) is more focused on what to do when individual systems go down. It involves a hierarchical checklist of scenarios and responses that will be your playbook, should disaster strike. Broadly speaking, the steps you should take follow this framework: stop the bleeding, patch the wound, assess the damage and take remedial action.

Step 6: Run Your Security Program

The last step is the one that never ends: running your new security program, without pause, while updating tools, training staff and modifying your BRP and DRP plans as the cyber landscape evolves. Day to day operations is the most difficult of a cyber security program. Patience, stamina, discipline and humility are the prerequisites.

Can You Keep Up?

THE RCMP IS STRUGGLING TO KEEP UP. THINK YOU CAN?

In September, 2018 the RCMP revealed that it is having trouble keeping up with cybercrime because of the prevalence of online encryption[13] and because of sheer volume. If the RCMP can't keep up, how can you expect to?

Luckily, sheer volume and encryption of information are not factors that most businesses have to deal with. Many large organizations are doing a great job of repelling attacks, the Big Five and the federal government in particular. Both invest millions of dollars per year on their cyber security program.

THE FINANCIAL CONSEQUENCES OF A SECURITY BREACH

$2.4 million

The average cost of a malware attack on a company is $2.4 million[14]

61%

61% of breach victims in 2017 were businesses with under 1,000 employees[15]

When organizations reach the point at which they can bring a strong cyber defence program in-house, most have ceased to be SMBs. Keeping up takes deep pockets. But think of it this way: what is it worth to you not to suffer the financial burden of a cyberattack? Again, our best advice is to prepare for a breach according to the impact on your business. Calculating the ROI of a cyber security program is not complicated. Add up the cost of downtime + cost of recovering data + the cost to your reputation/competitive position and multiply that figure by the threat you face of a breach, expressed as a percentage.

[13] Catherine Tunney, "RCMP's Ability to Police Digital Realm 'Rapidly Declining,' Commissioner Warned," CBC.ca, September 24, 2018, accessed September 2018, https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340.
[14] Rob Sobers, "60 Must-Know Cybersecurity Statistics for 2018," Varonis May 18, 2018, accessed November 2018, https://www.varonis.com/blog/cybersecurity-statistics/.
[15] ibid

What's Next?

Quartet's Managed Security Services integrates a wide range of tools and processes into a comprehensive cyber security defence platform. This includes 24/7 monitoring, phishing campaign recognition and training, disaster recovery plans and much more. To get you started, we use three steps:

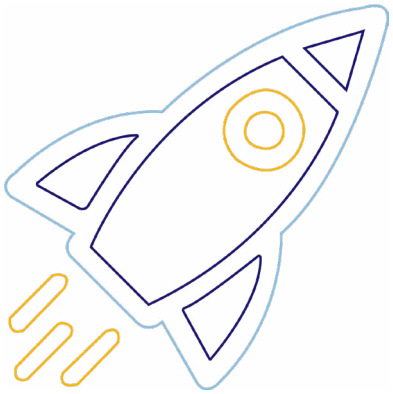
Step 1: Environmental Audit

We'll do a current state analysis with network, server and security consultants to show the strengths and weaknesses in your system.

Step 2: Visionary Budget

Next we'll create a budget and project plan for your organization. All initiatives will have a business case and will be ranked into must do, should do and could do.

Step 3: Launch and Maintain



Finally we'll launch your program. We'll organize monthly meetings that include progress reports and detailed performance feedback statistics. We'll enhance your cyber security position and provide day-to-day support to ensure operational compliance and efficien-

What's Next?

Evaluate your cyber security position from a wholistic standpoint. Your security posture is only as strong as the weakest link. This process usually includes 3 steps:

Step 1: Align

Evaluate each layer of your technology stack. We use a 300 item checklist to identify risks and prioritize recommendations.

Step 2: Survey

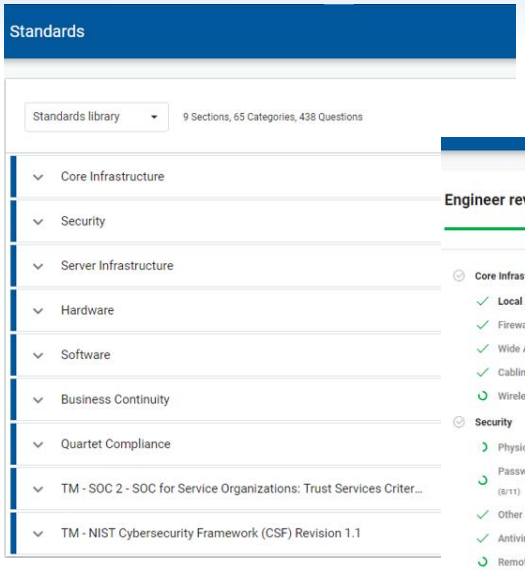
Survey your management staff to evaluate your cyber security awareness, processes and policies.

Step 3: Plan

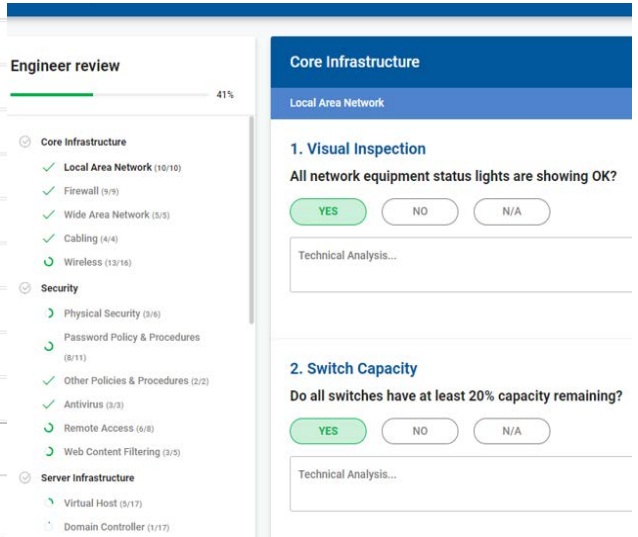
Build a strategic cyber security roadmap to track milestones, budgets, timelines and performance.

A disciplined discovery process ensures that information isn't missed and builds internal consensus for change. The discovery process will help explain cyber security initiatives to boards of directors and senior management.

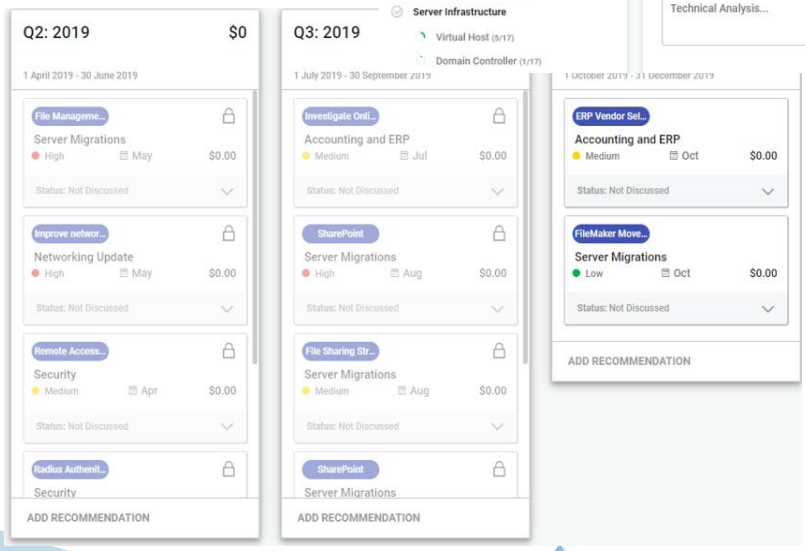
Step 1: Align



Step 2: Survey



Step 3: Plan



Quartet Can Help

We Help Strong Toronto Companies Stay Strong.

We've been helping Toronto companies maintain efficient, secure IT environments since 1998. We play the long game. An effective IT strategy isn't a one-time deliverable; it's a constantly evolving execution, shaped by the kind of risk your business faces, efficiency and ROI.

In 2017, we became SOC2-compliant, meaning that we conform to strict, audited standards of secure data management that protect customer interests and privacy. That's just the latest in a long string of investments we make on behalf of our customers. When we acquire new tools or certifications like SOC, all our customers benefit. The same is true for our IT security services and solutions: we conduct the cybersecurity audits that most auditors now require of customers like ours. We also help clients transform their security posture to a robust security information and event management (SIEM) approach. The bottom line is simple. If it's something we think you need, we'll make sure you have it.

Let Us Join Your Team

To find out more about Quartet, call us at +1 416-483-8332 or email talktous@quartetservice.com.

www.quartetservice.com

quartet

Do You Conform to the Digital Privacy Act?

Effective as of November 1, 2018: mandatory breach reporting regulation for all businesses that are subject to PIPEDA.

quartet

Let Us Join Your Team

Quartet Service Inc.
500-214 King St. West
Toronto, ON
4164838332
talktous@quartetservice.com
www.quartetservice.com