XRATOR
CONQUER YOUR RISK

RESILIENT GROWTH

Preventive Cyber Security Strategy Guide for SMB in Singapore

François MOERMAN
CEO at XRATOR

Our goal is not to detect and block cyber-attacks. It is that the attack can’t even happen in the first place.

> *Proactive risk management avoids damage that can't be fixed by detection & response alone. It is easier to get insured.”*

The price of preventive measures is low compared to the price of reaction after the damage has occurred.

Tech-enabled Growth

Digital transformation improves capital and labour utilization. By optimising productivity, operations and marketing costs, small businesses can reduce their overall expense while improving their margin. The MIT Centre for Digital Business claims that businesses that have embraced digital transformation are 26% more profitable than their average industry competitors and have a 12% higher market valuation (worldwide).

The shadow of cyber attacks

In the rush for digitalisation, SMB must integrate from the start cybersecurity to avoid disastrous consequences.
In 2021, 65% of organisations in Singapore were hit by a ransomware attempt (Sophos). 40% of SMBs suffered a successful cyber-attack with a medium cost of 700,000 SGD (NUS-ISS).
Singaporean Chief Security Officers are aware of this situation and have implemented cybersecurity detection tools such as Antivirus, EDR and IPS.
The result is that 44% of them witnessed an increase in Advanced Persistent Threat (« APT ») that create tailored attacks to avoid detection technologies (Proofpoint).

Cyber Risk is a Business Risk

Most of organisations start by investing in detection technologies. But detection tools such as antivirus mean the attacker already jumped the fence. If the attack was blocked, it is a matter of time before they come back and succeed. It is no secret that the hike in ransomware assaults is a serious concern

for business operations and cashflow.
In business we accept risks every day. We know that whatever our effort and commitment, failure can happen. So, we prepare several plans, setup layered strategy and prioritize where our efforts have the most value and chances to succeed.

Adopt Preventive Security

This business-oriented mindset in commercial operations is exactly the one we must adopt for cybersecurity.
Being proactive in understanding the market and the customer is how we create successful products or services. And seasoned businessmen know that their first and most reliable tools are employees.
Preventive cybersecurity is understanding the threat landscape instead of the market, mastering your security posture instead of your portfolio and knowing intimately your adversaries instead of your customers.

It is a proactive approach that involves the commitment of the leadership before the use of tools. You identify where your Business Value lies in the technology and focus your effort and investment here.
Preventive Cybersecurity ensures to put the appropriate protection where it is needed and helps reducing detection technology costs.

Achieve Cyber Resilience

It is equally important to be shielded and to be ready to take the next hit. Cyber Resilience is the path where a successful cyber intrusion have little to no impact. You are back on your feet quickly and ready to dodge the next shot.

> "
> *While you must block all incoming strikes, attackers must succeed only once."*

Promote your Accountability

Given the high level of interconnectedness with internet, attackers can also pose a threat to the stability of the overall society. It is essential that all organizations have an adequate level of cyber resilience to ensure their own protection as well as that of the entire ecosystem.

Customers now value data privacy and cyber security very much. Demonstrating and promoting your proactive posture will help you to develop a competitive advantage, increase your customer base and open new regulated sensitive market.

François Moerman
CEO at XRATOR

Executive Summary

Economic globalization and interconnection

The digital revolution has affected all areas of life (businesses, governments, citizens, and so on) and has provided a new platform for communication and sharing of information: cyberspace.

Because of its role as a place where value is created, but also where exchanges and confrontations occur, cyberspace has become a place for social, technological, economical, operational, and political dealings. The rules of competition are being altered as attackers redouble their efforts to achieve their objectives.

Cyber attacks can exploit trusting relationships between stakeholders (e.g., a company and its provider) to inflict unpredictable and lightning-fast harm on organizations. Sometimes these attacks are fatal.

From technical risk to business risk

For many years, companies and local authorities have implemented IT risk management that focuses solely on the security of their information systems. This was based on criteria such as confidentiality, integrity and availability that applied mainly to cross-functional or support activities.

All of society's players are now using digital technologies to perform most of their business functions, and their connections have grown. As a result, IT risk management evolves into a global management of digital risk.

Cyber Risk Management Challenges for SMB

One of the main reasons small businesses delays preventive cybersecurity initiatives is due to a lack of resources. There simply isn't enough money, time or people to properly run such a program.

Then, the more types of risk you have to deal with, the more complicated your risk management process will be. Business Impact Analysis, Security Compliance, Vulnerability Mitigation, Employee awareness.

Another major pain is the difficult communication between Business Leader and Technical Expert. Even with good faith one does not seem able to put themselves in the shoe of the other. This leads to blurred reporting and useless performance indicators.

Finally, shop around for the best and cheapest strategy. Our preventive strategy is costless compared to the cost of reactive tools and damage costs.

Agenda

1 Plan your risk strategy
2 Build your baseline
3 Set up governance
4 Design your budget
5 Protect data privacy
6 Get government funding
7 Your path to resilience

Key Takeaways

Be prepared: engage top executives ready to lead the fight back when attacked.
Prioritize: create the minimal security baseline around your critical assets.
Be a leader: create a map of your riskier operations and design KPI to steer the continuous improvement.
Save money: learn how to lower your cost by adopting a preventive strategy.
Be compliant: demonstrate your accountability to customer and regulator.
Get funding: get your money back quickly by investing in preventive cybersecurity.

This guide offers a step-by-step approach to turn any SMB into a cyber-resilient organization. You will gain a deep business-oriented knowledge with cybersecurity principles. If you already have a strategy in place, you will also find useful tips and resources to strengthen your Security Posture.

1 Plan your risk strategy

Create a cyber risk committee

A dedicated committee is required to define an organization's cyber security strategy in line with business priorities. It maintains, monitors and reviews the performance of the investment.

Define the Governance Framework

The committee is responsible for developing a digital security strategy that is up-to-date and accurately reflects the current digital risks to the organization's activities.

At least one senior management representative, one business development representative, and one member of each Business Unit are part of the committee.

Understanding the Mission

The purpose of the Committee is to free the senior leadership from existing functional, business and operational silos. Digital transformation is cross-functional and the approach to secure it is global.

Those risks are not limited to the organization alone but also concern the stakeholders of the value chain. It is essential that the committee chairman is a senior executive to ensure the business alignment, to facilitate quick and independent decision and to assert the leadership toward a global organization security culture.

MISSION CHECKLIST

- ☐ Create and maintain the organization's Security Policy that governs the risk management.
- ☐ Priorities and define the investment to enforce the Security Policy.
- ☐ Prioritize the security of the most critical digital services.
- ☐ Drive the Performance Review and the Security Continuous Improvement Plan.
- ☐ Define a valorization strategy of the security investment to increase the company valuation and competitiveness.

Identify your crown jewels

A critical asset (also called Crown Jewel) may be a piece of equipment, a data center, or a person who has specialized knowledge and skills. The loss of a critical asset could have serious consequences for the company, such as the inability to operate or to meet customer needs.

Critical Asset Identification

A key example is an ERP system (Enterprise Resource Planning). In the event of a cyberattack, the ability to access and share critical data across all departments is essential to the ongoing operations of the company.
If the ERP is compromised, the entire business can be jeopardized. A strong cyber security program is essential to protecting these assets.

> *The identification of critical assets is the major step to develop a cybersecurity strategy."*

Once the assets have been identified, appropriate security measures can be put in place to protect them from attack.

Critical assets may not be the same for senior leadership and for IT experts. Both need to work together. The final goal is to protect the organization, not the technology.

Critical Assets Selection

To begin, the cyber-risk committee should not aim to cover everything, but rather identify the key digital services and systems, and identify which ones will receive extra attention. This high-level of detail is sufficient to construct worst-case cyber-risk scenario and identify the assets that the committee should focus on.

ASSET INVENTORY

Critical Asset: XRATOR SaaS automated asset scanner discovers all the asset of your network. You can organize them by Business Unit and quickly identify your Crown Jewels.

Security Baseline: XRATOR Scanner contains best practice assessments and a remediation database. You can check your security baseline with a click and improve it.

Build your worst-case risk scenarios

A cyber attack scenario can point out the existence of an information system (internal or external) that was previously unidentified as a critical system.

The strategy begins with identifying and quantifying the most critical cyber-attack scenarios to the organization, combined with a best practice compliance approach.

Best Practice Approach

The prevention of the most common cyberattacks on information systems can be quickly achieved by respecting standards and best practices.

By implementing and monitoring the compliance-driven minimal security baseline, an organization can refocus its risk analysis efforts on the most critical scenarios for the business.

Building Worst-case Scenarios

Basically, the Cyber Risk Committee must work on four questions to elaborate their scenarios:

- What event can impact my critical asset ?
- Which attackers are likely to harm the organization's operation?
- What are attackers’ motivations ?
- Can my Information Systems resist to a carefully targeted attack ?
- What are the third-party risks that can impact the organization (risk of negative image, non-conformity, health, environmental, etc.)?

Critical cyberattack scenarios Selection

The Cyber Risk Committee creates scenarios of cyberattacks that could severely impact one or more of the organization's vital functions.

The level of risk is then defined according to the severity of these impacts and the likelihood of these scenarios. Likelihood reflects the degree of feasibility or possibility that an attacker will succeed in his objective. The effort will be put on the few top risk level.

Risk Scenario Quantification

Risk treatment options and priority can be informed by quantifying the financial impacts of the most critical cyberattack scenarios.

To calculate the cost of a successful cyber attack scenario, a financial analysis can be conducted taking into account the following elements:

- Contractual penalties with third parties;
- Legal and regulatory fines;
- Operating and production losses;
- Loss or destruction of essential information;
- Remediation of information systems;
- Business recovery.

However, some costs are difficult to estimate. These include the damage to the image, or the loss of consumer confidence caused by a product recall.

An organization can calculate the cost of such impacts by using an information intelligence strategy. It will be able to recognize the costs of similar-sized and similar-activity organizations experiencing cyber attack.

A scenario's specific details can be described in different phases: crisis, recovery, and improvement. List the parties affected and assess the financial implications at each level.

Be diligent with your estimation. Senior management's decision making on strategy direction is dependent on the financial estimates' credibility.

Risk Scenario Response

Technical experts are required to build a response. They will identify plausible intrusion path and offer mitigation measures. The goal is to reduce the likelihood of the scenario.

EXAMPLE OF RISK SCENARIOS

Business Unit	R&D	Sales & Billing	Production
Scenario	R&D files are stolen, and a competitor creates copies	Unavailability of the invoicing system	Unavailability of the production line
Impact	Financial Impact Reputation Impact	Financial Impact Reputation Impact	Financial Impact Reputation Impact
Estimated Loss	30% of annual revenue	20k SGD / day	35k SGD /day
Severity	Catastrophic Impact	Serious Impact	Catastrophic Impact
Likelihood	Plausible Scenario	Plausible Scenario	Very Plausible Scenario
Protection	Data Encryption & network isolation	Outsourcing for business continuity	Insurance Policy
Cost	25k SGD	3k SGD / day of crisis	10k SGD / year

Security posture as a competitive advantage

Since digital transformation has led to the emergence of new stakeholders, these stakeholders expect the organization to go beyond basic cybersecurity and to truly position itself as a trusted digital third party.

Cyber Maturity Benefits

Signing a contract with a large company can be a turning point in the life of an SMB. But these contracts are increasingly subject to their third-party security diligence.

By demonstrating and proving your level of security, you ensure the continuity of your key contracts. You can even approach new prospects who were previously too cautious to deal with you.

You can differentiate from the competition by bringing the business ecosystem value other that financial: trust, proactivity, investment optimization. Those are key to succeed in our ever evolving and volatile modern world.

Ecosystem friendly

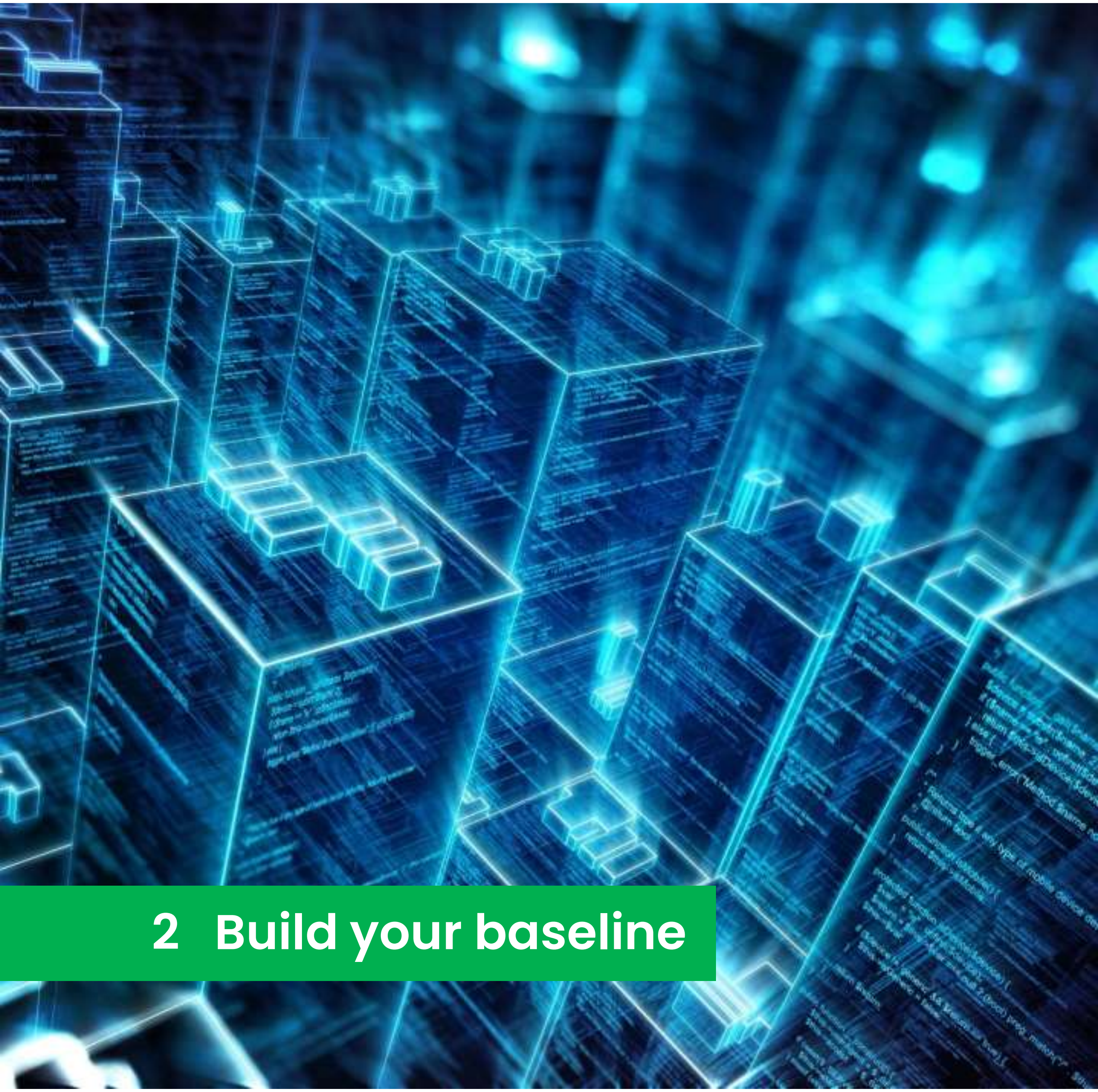
To meet the risk tolerance threshold of its customers, a SMB can provide the assurance of a cyber maturity compatible with their needs.

As a result, the organization can rely on this valuation as a statement to:

- Generate growth and seize opportunities from its ecosystem
- Apply to, rationalize or optimize Cyber Insurance Policy
- Unlock new market among customers that looks for security and trust as first criteria

By implementing this approach together with a communication strategy, the organization will influence the level of cyber maturity of its ecosystem, reduce cyber risk induced by third parties and improve its brand image.

> *Organisations must be able to anticipate the future expectations of customers, regulators and investors when it comes to their ability to manage cyber risk and provide guarantees.*



2 Build your baseline

Start with the human factor

Humans are both the creators and the users of the information system. As a central factor, they are the priority target for adversaries. Investing in people reduces the attack surface, increases adherence to the project and the rules, accelerates results and reduces technological costs.

Awareness and Training

Give the right dose of information and skills that applies to the specific job position. It must be renewed regularly regarding the evolution of the risks, the company strategy and the turnover. Hiring and keeping specialists must be a strategic priority.

> *An efficient training program allows internal carriers, junior hiring, reduces expert turnover in a skill-short market."*

Federate Stakeholders

The commitment of the employees and stakeholders in the organization's strategy is mandatory. Ideally the one of your third-parties too.

Attackers can exploit the trust relationship you have with a customer or supplier.

For example, if a supplier is hacked or impersonated, the attacker can use their credential to send you fake invoices with rogue bank account information or a malicious software.

Engagement as KPI

The engagement of employees in the defense of the organization must be regularly measured through internal surveys and questionnaires. An employee's reluctance is a weak signal of demotivation or a lack of understanding of the strategy.

EMPLOYEE HARDENING

Phishing Simulation: XRATOR scanners allow you to set up phishing simulations to train your employees’ acuity to spot an attacker trap.

Knowledge Quiz: XRATOR allows you to perform quiz campaigns testing your employees’ knowledge and score their progress.

Preventive and reactive measures

Security measure protects the business and its assets. It is the meeting of organizational, physical and digital processes. The protection needs way more than just IT skills.

Legal

An active contractual prevention policy must be deployed to not be exposed to prosecution, sometimes criminal, by clients and partners, regardless of their nationality. Integrate contractual clauses regarding cyber disruption to define requirements and responsibilities.

Digital usages

The professional and personal use of IT resources, business trips or access to wireless networks are risks for the organization's information system. It is advisable to anticipate these situations in order to reduce its exposure to such threats.
Define a security policy in line with the organization and the moderns' usages (BYOD, home office, …).

Business Projects

Business evolution must consider digital security early in order to avoid constraining the project with heavy security measures.

Agile methodology for integration of into projects is ideal.
Security must be integrated in every business evolution, as soon as the design phase.

Agile methodology for integration of into projects is ideal.
Security must be integrated in every business evolution, as soon as the design phase.

Physical Security

Digital risk involves controlling the physical environment and premises. Physical access control to the most important systems must be enforced, and a video protection system should be associated with it.

MATURITY BENCHMARK

Framework: XRATOR contains leading security frameworks, such as ISO27001 or NIST 800-53 that will guide you implementing those measures and benchmark their maturity.

Defending the network

Defending one's organization and activities is orienting countermeasures to ensure the failure of any critical scenario. As you evolve in cyberspace, your only way to see what happen is security logs.

Cyber Attacks Detection

The first and foremost duty of a detection resource (Firewall, proxies, IPS/IDS or antivirus) is to focus on the paths and techniques used by the attackers during the occurrence of a worst-case scenario.

Capitalize former incidents, external cases and use red teams to discover the plausible attacker's path of intrusion: entry points, pivoting points and final targets. This will help the Chief Security Officer and Chief Information Officer to put detection probes where it matters the most.

Logging and correlating

A line of log is like a strike of light in your retina. Without it, you are blind. Collection, storage, retention and correlation of logs allow to get insight on ongoing attacks.

A logging system should also be installed to preserve crucial information about when, where, and how users access sensitive data. These events and logs are then correlated to track, analyze, and generate appropriate security detection rules for the Security Operating Centre (SOC).

Cyber Attacks Qualification

Qualifying a cyber attack consists in identifying the activities and assets affected by the attack and, above all, the severity of these impacts. It is then a matter for the incident response team to react, treat and classify the incidents.

Identifying targeted assets and activities allows to priorities responses. Those responses are ideally formalized with cheat sheets and procedures, that define who must act, when to escalate to and trigger the crisis cell, and how to capitalize knowledge.

RED TEAM

As part of XRATOR White Gloves Services portfolio, our Team is expert in Red Teaming to helps you identify hidden and plausible path of intrusion.

Crisis and resilience

Cyber defenses are not the only one to deliver the proper response. Other actors and behaviors reinforce the capacity of an organization to preserve critical objectives even under siege.

Crisis Cell

A serious disruption activate the crisis cell that must reduce the impact and confine the propagation. It can trigger the BCP if the incident reach a pre-defined threshold.

Business Continuity Plan

The BCP is a procedure that organizes the operational reboot with minimal losses. It is based on critical scenarios and must be tested and readjusted regularly.

Business Recovery Plan

The BRP is a technical, operational and organizational procedure to reboot the business as soon as possible.

Crisis Communication

Inside the crisis cell, it delivers internal coordination and communicates externally to preserve reputation.
External crisis communication are prepared in advance. During the crisis, you have no time and you a not in shape to create reassuring and convincing communication.
Proactively, to each worst-case scenario, prepare your declaration to the public.

Law Enforcement

Every attack is a crime. Authorities can give advice and assistance, acting as a neutral actor.

You can ask the Singaporean government agency SingCERT's tool called Cyber Aid to diagnose your incident and get recommendation: www.csa.gov.sg/singcert/cyber-aid

In addition, you should fill a police report at: eservices.police.gov.sg, if you think you may have been the victim of a cybercrime.

ABOUT PDPA

If the breach is likely to result in **significant harm to affected individuals** to whom the information relates or if the breach is of a significant scale involving personal **data of 500 or more individuals** your need to notify the Personal Data Protection Commission.

3 Set up the governance

Performance and continuous improvement

The organization is adapting faster to new threats by integrating its digital risk management strategy process with an improvement approach. It strengthens its security base and controls its investments.

Audit & Control Strategy

An effective audit and control strategy ensures that the security level is maintained in an ever-changing environment. An audit examines the organizational, digital, or physical security measures to determine if they comply with regulations and Best Practices.

Security points of vigilance and non-conformity with respect to a reference system are identified by audits and controls. Those points define the Security Continuous Improvement Plan (SCIP).

> "
>
> *The control and audit strategy should be re-evaluated at regular intervals in order to account for changes in the organization and its environment."*

Continuous Threat Adaptation

The continuous improvement process supported by a Cyber Risk Committee must be based on:

- A media watch strategy;
- Indicators & Dashboard;
- The results of control and audit actions.

Thanks to the knowledge of new threats and the company's objectives for digital security, as well as the correction of non-conformities, the strategy can adapt dynamically.

CYBER POSTURE

Documentation: XRATOR centralizes Compliance Self-Assessment, Vulnerability Assessment, Reporting, Threat Feed and Document versioning.

Single Source of Truth: With XRATOR you have everything in hand, in a centralized place, to engage in a Security Continuous Improvement Plan (SCIP).

Driving performance

Measurement tools, such as indicators (strategic, governance, operational, organizational, or technical), are required for the Cyber risk committee to effectively manage digital risk. In order to fully take advantage of these data, they may then be integrated into dynamic dashboards in order to obtain a visual representation of the objectives and thus highlight trends or deviations.

EXAMPLE OF SECURITY KPI

Strategic Concern	Governance Response	Operational Response
State of the risk governance	- Frequency of Cyber Risk Committee meeting - Frequency of Compliance Assessment - Number of exceptions to the security policy	
State of the Cyber Risk	- Risk analysis rate on new projects - Number of open non-conformities - Rate of risks coverage	- Rate of vulnerable critical assets - Rate of vulnerable regular assets - Average time of remediation
State of the Incident Response	- Number of closed incidents - Number of open incidents - Average business interruption time	- Number of detected attacks - Availability rate of critical assets - Incident rate by Business Unit
State of the Documentation	- Review frequency of Security Policies - Review frequency of Security Procedures - Coverage ratio of published documentation	- Number of new security procedures published - Effective review ratio
State of the Awareness	- Awareness coverage ratio - IT administrator skill maturity - Number of crisis simulation	- Employee awareness certificate - Administrator Training certificate

Nine questions for board members

Cybersecurity and Cyber Risk Management ensure that the organization can exploit the full potential of technologies. Those topics are then strategic to an organization's resilience. The decision-making and support place the discussion at the Board level.

How is cybersecurity embedded into our strategic structure ?

Cybersecurity is an enabler of an organization's overall objectives. It impacts every aspect of this organization. It must then be integrated into the senior executive level discussion, decision-making and in the organizational risk management.

Good cybersecurity is not just having sufficient budget or the best technologies. It is first a human factor topic. Build healthy relationship with cybersecurity goes by a top-level support, an integration into the organization culture, building the right process and manage them.

How do we manage security expertise and human resources ?

Cyber skills are in very high demand.

Today it is expected that the cybersecurity workforce should grow by 65% to meet the defense needs. Organization must take steps to ensure they can attract and retain cybersecurity expertise.

The solution involves the creation of internal program to build skills in-house, listening to the workforce demands to build an attractive employer image and outsource specific functions the organization trusts to be able to monitor.

How are we building a positive cybersecurity culture ?

Cybersecurity can be seen as a burden for those who must enforce the rules in their day-to-day job. It makes their tasks heavier, with no reward and raising concerns may equal to get into trouble. People must feel safe to raise concern and to challenge ineffective practices.

Putting people at the heart of the strategic structure and policies enlights them about the “why” and “how”. Focusing only on technology will increase the risk to overlook the needs of people to perform their duty securely. It generally results in the creation of dangerous and hidden shortcuts that create new cybersecurity risks.

What are our Crown Jewel ?

Understanding what technical assets are key to achieve the organization's objectives is mandatory for an effective cyber risk management strategy. Like any Business Risk, it is impossible to mitigate all cybersecurity vulnerabilities. The defense has to be prioritized.

Technical experts need the support of Top Management and Business Practice to protect the organization essentials. They must be provided the suitable tools and channels for communicating their advises, as well as the level of organization the Board needs to take decision.

Who are our adversaries ?

Too frequently when talking about cyberattacks, the "Threat" is seen as a kind of technical abstract entity. Cyber Threat are People. They can be a lone wolf hacker or organized group; they can target a precise industrial segment or act in an opportunistic manner.

Understanding the organization's threats requires first to understand what is valuable in the organization. We do not face the same criminal predation depending on who we are. The prioritization of the defense also comes by screening the cyber adversaries and focus on the one hitting the strategical structure.

How are cyber security and risk management aligned?

As cybersecurity is born among technical teams and risk management is tied to high management, the first is generally subordinated to the second. It is a huge mistake. Risk Management generally focuses on meeting compliance standards. Cyber Threat don't care about compliance standards.

The most effective cyber risk management must build the minimal security baseline on industry and regulation requirements. Then one can use this foundation to create cyber risk scenarios and explore the systemic consequences of cyber disruptions.

How effective are our cyber security measures ?

Implementing good security measures is mandatory to meet regulatory requirements. But it foremost helps the organization to meet strategic objectives and reduce the likelihood of significant incident. You can't avoid cyberattack attempts, but you can reduce their impact.

While building the security baseline, the security control baseline must be implemented at the same time. It means setting up technical metrics aligned with the organization's objectives and missions. Using recognized frameworks such as ISO27001 or NIST800-53 is a good place to start to mitigate the highest priority risks. When the needs and the threats of the organizations evolve, you will have to create your own controls to assess if defenses are still effective.

How do we collaborate with Third Parties ?

Every organization is part of a Global Value Chain. It may have implemented the best security culture, but sometimes the problem comes from the outside. Cyberattacks on your Third Parties can be just as damaging as if you were the target.

Cybersecurity practice and Cyber Risk analysis must be included in any decision about a new strategic collaboration. Among the most critical, investing, merging or acquiring a third party must include in the due diligence a cybersecurity assessment of their network.

How is our cyber incident response planned?

Cyber incidents have a direct impact on an organization's budget, productivity and reputation. In time of crisis some hierarchical layers must be taken apart to ensure a seamless dialogue between technical experts and strategic decision-makers.

As an executive, to be prepared to respond to a cyber-attack contains damage-control, reducing the financial impact and managing disruption. With the media interest into cybercrime, the Board must also manage the external and internal perception of the management of the attack to preserve their reputation.

DIGITAL IS STRATEGIC

Impact on reputation, on operations, new regulation such as Data Privacy Laws have raised the expectation of customers, investors, regulators and the wider public when it comes to cybersecurity. It is now a mandatory features for any organization.

4 Design your budget

Budgeting in the era of digitalization

When you set up a conquest strategy, you design your budget to fit with the objectives, not the way around. Yet, the current line-item strategy of CFO demands the winning cybersecurity strategy to match a predetermined budget.

Budget is a tool to achieve objectives, not the contrary

A company leadership must evaluate what is needed to be protected. If one of your Crown Jewels is at risk, if your new digital marketing campaign has not been evaluated, it is your priority to design the counter-measure plan and then evaluate the appropriate budget to meet your strategic requirement.

Companies don't have infinite budget line. It is then even more important to carefully put your money where it has the most impact. Understand your business environment, assess your Threat Landscape and plan your risk mitigation strategy where it is has the most impact.

Prepare the mindset before the budget

Every Business Holder knows that when you throw money to an unprepared project, it can't end up other than a failure. Before allocating money to a cyber risk management line, senior management must ensure than all stakeholder understand and support the current strategy and priority.

The cybersecurity mindset alignment require to identify the key stakeholders across the business lines. Finance, IT, HR, Sales. Infuse the mindset into your chain of management, gather cybersecurity champions that will support the strategy and finally design the necessary budget.

Benchmark your Cybersecurity Budget

Cyber Risk and Cybersecurity Governance are mastering the use of Framework. Will it be NIST Cybersecurity Framework, ISO27001 or COBIT, all those tools split the security topics into a few key areas. Are you more savvy at risk prevention or attack detection ? Is your Threat Landscape heavier on social engineering or technological attacks?

Interactions between senior management, governance and technical experts help you to weight those key cybersecurity area in term of maturity and risk. It is your compass to design an equally split budget into three types of actions for a reliable cybersecurity:

- Quick wins: easy and cheap actions that have a visibility impact you can leverage for commercial purposes
- Infrastructure: maintain, refactor and upgrade your current security measure
- Strategy: implement your new cybersecurity objectives.

The current way of working of CFO and budgeting is reactive. You unlock a cybersecurity budget after you have been hit by a cyber-attack. You may go away with it a few times. But information technologies are now a key factor of value creation in our interconnected world. A single cyberattack can lead to bankruptcy.

Start small key investments, build a minimal security baseline based on Best Practice and create a cybersecurity culture that will make your company resilient. Adopting a proactive approach to cyber risk budgeting will also, on the long run, decrease its overall cost.

TRAPS OF TIGHT BUDGETS

A tight-budget SMB may be tempted to outsource all its IT security to external providers. You think everything is under their control and you have a fixed budget.

The problem is that these company only take care of the reactive cybersecurity. In case of a problem, you will be responsible in front of your customers and regulators.

Using a platform like XRATOR SaaS reduces the number of licenses you pay while giving you the upper-hand decision. With our Compliance Benchmark you are better informed on what protection and services you need from an outsourced IT provider. You can then cherry pick interventions and lower your previous expenses.

Inexpensive cybersecurity measures

A business starts to be at risk as soon as it has an email address. Developing from the start an aware and honest vision about all business aspects, including predation and malicious actions, is key to thrive in entrepreneurship.

Train your employees first

Small companies will generally rely on multi-role and agile employees. They can't afford at early stage a full-time cybersecurity specialist. Turning every employees into a cybersecurity chain link will greatly reduce the attack surface. It also reduces the time needed to detect and respond to a disruption.

As 80% of cyberattacks involve social engineering (IC3), employees that yield responsibilities on their own devices will help to implement a healthy cyber-accountable culture. No need to spend a lot of money and time in it. Ask your employees to spend a little time of research in their own perimeter to then share it to everyone.

Keep your software updated

When attacking software, most cybercriminals will target known vulnerabilities that have been patched by a vendor update.

Whether it be laptop operating system, mobile application, webserver, update notifications should not be perceived as annoying: they are here to help.

If it is possible, enable automated updates. Include in your employee awareness session the habits to install them as soon as they appear.

Ignoring those notifications is giving away free cybersecurity and increasing your cyberattack surface.

Prioritize your Crown Jewels

Not all your information and processes have the same business impact. At first you may think that you need to protect everything. But after a few question to C-Levels, a CTO can identify a handful of equipment, process or information that are truly making the start-up successful.

Trained employees, updated antivirus and software create your first and minimal security baseline. You can spend your little cybersecurity budget to implement additional protection around those Most Valuable Assets: backup, penetration testing, physical security.

Manage your Identities and Access

Minimize administrative privileges and access to sensitive documentation.

Having a healthy relationship with user accounts will also help to identify obsolete ones. Those accounts created months ago for a trainee now out of the company, or this administrator account created just for the launch of one project. Those forgotten accounts are what cybercriminal are searching for. Get rid of them.

Protect your showcase website

Internet presence is key for successful SMB. They may spend thousands of dollars in Web Agency, copywriting or Search Engine Optimization. But none in cyber protection. If your website is down or defaced, your business can go down in a matter of hours.

Cheap web security offered by players like Cloudflare, Akamai or Imperva are available for a few tenths of dollars a month. They will act as a proxy, filtering the internet traffic and trashing Web Attacks, DDOS attacks and spamming bots.

ALL IN ONE

Employee Training: XRATOR SaaS phishing simulation trains employee to spot social engineering attacks. They learn by practice, and you get KPI to see your improvement over time.

Software Update: XRATOR SaaS automated scans give you a complete view of where software need to be updated.

Crown Jewels: XRATOR SaaS asset manager allows you to highlight and track your Crown Jewels security.

Identity & Access: XRATOR SaaS asset manager highlights and tracks your privileged account.

Showcase Website: XRATOR SaaS automated scans deliver remediation for vulnerabilities and configurations mistakes that attackers use to take down your business.

Reduce your cybersecurity costs

If you find yourself spending too much time, money and resources on cyber security management, it may be time to reassess your current strategies and explore other, more cost-effective options.

Change your mindset

A lot of businesses out there tend to treat cyber security as an expense. Instead, you should begin viewing cyber security as an investment. Implementing new strategies and technologies to enhance your current security measures can help you prevent data breaches, data loss and other cyber incidents that can lead to significant losses.

If you approach cyber security as an investment, you may be more likely to allocate funds to the right areas and be able to reduce your cybersecurity budget in the long run. Additionally, when you view cyber security as an investment, you may be more likely to prioritize it as a higher priority compared to other expenses. This can help you take the necessary steps to improve your security posture.

Use Automation

The major component of the cyber security cost is the skilled workforce that is hard to find and expensive due to a limited talent pool.

Automate the Cybersecurity requirements of your company. It will greatly reduce the labor costs. Additionally, it will also be faster, efficient and reliable

There are many technologies and tools out there that can automate certain tasks related to cyber security and help reduce time and effort. For example, auditing software such as XRATOR can help you automate and streamline the process of auditing your network and identifying potential cybersecurity threats.

While automation and machine learning may seem like a good idea, it’s important to note that these solutions may not be able to replace human intervention. For example, when it comes to developing security policies, businesses often prioritize getting the process completed as quickly as possible. For this reason, some organizations may choose to automate this portion of the process. However, it’s important that you don’t skip any important steps and that you get a security policy written by a human. This will help ensure that your policies are as effective as possible.

Consolidate your services

Another way businesses can reduce the cost of their cybersecurity efforts is by consolidating their services with one provider. If your company uses an on-premise firewall, separate IDS/IPS systems, antivirus software and other security solutions to protect itself from cyber threats, it's likely that you're spending a substantial amount on these services each month.

To reduce your costs, you can seek out a single provider that offers a variety of security solutions. This can include a managed firewall service, an intrusion detection and prevention system, antivirus software and more. By finding a single vendor to partner with, you can save money and reduce the amount of time and effort spent managing each of these separate services.

> "
>
> *Change your mindset and view cyber security as an investment, then prioritize your resources to prevent cyber threats and reduce costs at the same time."*

COST FRIENDLY

Business Alignment: XRATOR SaaS Business Impact Analysis engages decision-maker in a quick process to spot their most profitable yet vulnerable business line.

Core Automation: XRATOR SaaS has automated asset discovery, IT vulnerability scanning, phishing simulation on employees and even report generation. You just need to click, and it's done. No more costly outsourced audit.

Policy Templates: XRATOR SaaS policy manager offers you a set of templates for all your policies, guidelines and procedures.

Consolidation: XRATOR SaaS integrates in one single tool Governance, Compliance, Asset Management, Vulnerability Management, Project Management and Reporting.

5 Protect data privacy

Doing business in the 21st century in Singapore

In 2019, The Personal Data Protection Commission (PDPC) indicated that 66% of customers preferred purchasing from a Personal Data certified company. The numbers rise to 80% of company that prefer doing business with a certified organization.

> "
>
> *Safeguard and enhance your corporate images, strengthen your position in the industry."*

How to get started ?
An organization must develop and implement policies and procedures necessary to comply with the 2012 Personal Data Protection Act (PDPA) if it collects, stores, uses, archives or discloses personal data.

A Data Protection strategy must establish policies and procedures to develop and improve personal data protection. The first step is to create a Data Protection Management Program (DPMP) tailored to their organizational needs.

As no organization is 100% safe from personal data violation, a Data Breach Management Plan (DBMP) must be developed and shared inside your organization. It allows your employees to read when a data breach occurs. It contains Standard Operating Procedures (SOPs), instructions detailing how to perform a particular task, step by step.

A contract that involves the exchanges of personal data by one of the parties, both of them, or external parties, may be included in the Service Agreement, for general reference. It details clearly the requirements for protecting personal data between two parties, outlines the procedures for monitoring compliance, and describes the steps to be taken in case of data breaches.

Finally, when an organization is designing a new process or introduces major evolutions in a process that involves personal data, a Data Privacy Impact Assessment (DPIA) is the tool to go. DPIA is very suitable when you start from scratch, as it allows you to define a data-centric risk assessment, to map your data flows. You can find DPIA templates on the PDPC website: https://www.pdpc.gov.sg

Develop a DPMP

An organization can use a DPMP approach to build a robust data protection infrastructure by identifying management policies and procedures for handling personal data as well as defining roles and responsibilities for individuals in relation to personal data protection. Data protection management, as defined by a DPMP, can demonstrate an organization's accountability.

Developing a DPMP revolves around four main steps:

- Integrate the data protection policy in the corporate governance to cover the direction and course of action to meet PDPD obligations;
- Distribute roles and responsibilities in the data protection initiative to individuals that deeply understand the organization, starting with the Data Protection Officer (DPO);
- Turn policies into processes to operationalize their data protection initiative;
- Monitor and update the performance of policies, process and people.

You can find more detailed information and guidelines on the PDPC website: https://www.pdpc.gov.sg

DPO APPOINTMENT

An organization must have at least one DPO to ensure that it complies with the PDPA. The DPO must be a senior management position. It may be handled by one employee, a group of employees, or outsourced, depending on the organization needs. If the DPO it outsourced, a person appointed by senior management must be its Point of Contact.

The individual acting as DPO must have a data protection-related job scope. The DPO is independent from Business Unit Managers and must have the same independence as corporate lawyers or internal auditors.

The DPO monitors policies and procedures application, advocates the personal data accountability posture to employees, informs senior management, handles queries, compliance and breach notification

Data breach notification

Personal data breaches can result in financial losses and eroded consumer trust for an organization. Individuals with compromised personal data can be vulnerable to significant harm.

Individual significant harm

The non-authorized divulgation of personal data can have dangerous implications for the individual. Anything related to financial and wealth information can lead to scam, blackmail, robbery or kidnapping.

Health and genetic data can be leveraged to blackmail people to publicly release the information. If the person is of high status it can put to the ground a whole organization.

Identifiers such as social security number, picture, identity card, postal address is easily turned by criminal into impersonation fraud. As a result, the data leak-affected individuals can be wrongly accused of perpetrating this impersonated fraud.

Identifier of minorities or political refugees can be used by malicious entities to track them down and put their life at risk.

Data leaks have disastrous real-life consequences.

Prepare for data breach

A data breach can happen for several reasons, so organizations should have measures in place to monitor and prevent them. It is important to identify data breaches as risk-based as well as design monitoring methods and remediation measures that are effective.

Data Breach Management Plans (DBMP) are critical since they help companies respond quickly to data breaches by systematically managing them. It is best to plan for data breaches early, since organizations without a DBMP will find it difficult and chaotic when confronted with an actual data breach.

The DPMP covers the following items:

- Definition of a data breach
- Internal data breach reporting
- Data Breach Response
- Management Responsibilities

In addition to data breach management plans, businesses may also develop crisis management, communications, and business continuity policies to help them recover from data breaches.

Respond to data breach
In the event of a data breach, each action must be tailored to the situation. Data breaches must be handled accordingly to four key steps: C.A.R.E.

CONTAIN - Activate the data breach management team to reduce the potential impact of a data breach.

ASSESS – Understand the extend and impact of the data breach to apply the appropriate procedure and eventually trigger a PDPC notification.

REPORT – If the organization notifies the PDPC, they can receive remediation guidance.

EVALUATE – organization should look at the data breach and recognize where it can improve its personal data handling procedures and avoid future data breaches.

Data breach Notification
An organization must take reasonable and expeditious steps to assess whether a data breach is notifiable under the PDPA within 30 calendar days after a suspected or confirmed data breach assessment. The organization must document all steps taken during the assessment to demonstrate their accountability to the PDPC.

A data breach is required to be notifiable if it is expected to result in one of the following criteria:

- Individual significant harm
- 500 or more affected individual

When an organization determines that a data breach is notifiable, it must notify the commission within three calendar day and affected individuals as soon as possible.

When notifying the affected individuals or the commission, the organization should provide any information to the best of its knowledge and belief regarding the data breach.

REFLEX CARD

Submit your notification at eservice.pdpc.gov.sg/case/db with:
Facts of the data breach
Data breach handling
Your contact details

Call during working hours for major incident: +65 6377 3131

Data protection certification

To increase their competitive advantage and build trust with their customers and stakeholders, an organization can voluntarily apply to the Data Protection Trust Mark (DPTM) certification.

Competitive Advantage

Consumers are more cautious about the protection of their personal data than ever before, thanks to the public scrutiny of data breaches and the heightened awareness of personal data protection.

By obtaining the DPTM, your company can demonstrate that it has a robust data protection policy in place to safeguard their personal data, enhancing its reputation and fostering consumer confidence and trust.

Accountability Recognition

A government-supported third-party gives internal assurance within your organization by demonstrating that current data protection procedures are valid and identifying possible flaws in those procedures.

Being accountable in managing personal data is a sound business strategy that strengthen brand reputation and customer trust.

DPTM CHECKLIST

- ☐ Self-Assessment: XRATOR includes a DPTM checklist to increase the chance of certification
- ☐ Data Protection Policy: XRATOR allows you to create, manage, improve and oversee all policies documentation
- ☐ Data Protection Procedure: XRATOR allows you to create, manage, improve and oversee all procedures documentation
- ☐ Employee Awareness: XRATOR allows you to test employees' skills and knowledge
- ☐ Data Protection: XRATOR allows you to spot vulnerability and weakness in your data systems.
- ☐ Overseas Transfer: XRATOR inventories your third-parties and scores their security reputation
- ☐ Accountability: XRATOR assign employees to roles and responsibilities

6 Get government funding

Cyber & data program grants

As part of the national strategy in Digital Transformation, Singapore's government developed several grant programs for SMB cyber security, cyber risk and data protection initiatives.

Productivity Solutions Grant

The Infocomm Media Development Authority (IMDA) has established a list of pre-approved, cost-effective and reliable solutions, making going digital for SMBs simple. SMBs that adopt these pre-approved solutions can receive funding support from the Productivity Solutions Grant (PSG).

Pre-approved solution make the investment eligible up to a 70% funding. For food and Retails SMBs the grant is up to 80% until March 2023. More information at: www.csa.gov.sg/programmes/psg-cybersecurity-solutions

Cyber Safe Grant

The Cyber Safe Certification promotes the Cyber Essentials mark. It is aimed at SMBs and is a cybersecurity certification. It means that an organization has prioritized cybersecurity protection as part of its cybersecurity transformation. Some SMBs may lack IT and cybersecurity expertise and resources, making the Cyber Essentials mark particularly beneficial to them.

SMB that are certified before March 2023 can receive government incentives that are deductible from the certification fees. They are also eligible for a cyber insurance at discounted rate. The next step certification, Cyber Trust, is eligible for the Enterprise Singapore Grant (ESG).

Data Protection Grant

Singaporean SMBs seeking to obtain the Data Protection Trust Mark (DPTM) can seek support for certification and consultancy services under the Enterprise Singapore Grant (ESG).

DPTM CHECKLIST

- ❑ **Asset:** XRATOR inventories People, Hardware, Software and Data
- ❑ **Secure:** XRATOR detects unsecure configuration
- ❑ **Update:** XRATOR detects outdated software
- ❑ **Backup:** XRATOR helps you manage a backup procedure
- ❑ **Respond:** XRATOR helps you manage Incident Response procedures

7 Your path to resilience

Positive adaptation during significant adversity

Historically, cybersecurity was based on a perimeter control model. The defense was passive and reactive, based on a generic detect-respond paradigm. In line with the industrialization of cybercrime and the consolidation of state-sponsored cyber-operations, organizations must acquire a dynamic logic to continue to operate their vital activities even in case of an attack.

Cyber maturity is not enough

Cyber maturity is the must-have baseline for any connected organization. But cybersecurity technologies are solutions controlled by third parties and may not follow the organization's needs. They may also lag the fast innovation pace of adversaries in their techniques and business model, such as the ransomware phenomenon.

The defender learning curve must increase with iterative learning. You prepare you strategy, you apply the strategy, you assess your KPI. Yet sometimes you still fall along the way. If there are no lessons learned about success and failure, an organization may have a good posture at one moment, but we can trust adversaries that it will not last for long. How to get back on track quicker ? How to muscle our ability to reassess our strategy ? How to accept that our plan focuses on the most critical point, but not all points?

Volatility, Uncertainty, Complexity, Ambiguity

At the end of the last century, a new raw material was created through communication technologies and data exploitation, establishing the foundation for the third industrial revolution. Towards the end of the current century, we are heading to a fourth revolution bringing together all the new technologies.

The world has changed dramatically. We now live in a physically and digitally connected, transformed society. Disruptions are fast-paced, constant and unpredictable. We are experiencing a state of turbulent flow rather than the assurance, stasis, and familiarity they were accustomed to.

The US military concept of VUCA seems to describes the taste of time we are entering:

- **Volatility:** the unexpected events we can act on with certainty
- **Uncertainty:** the plausible events we have no idea how to deal with
- **Complexity:** the entanglement of basics events making it hard to understand and take appropriate action
- **Ambiguity:** you don’t know that you don’t know how to act on this event

Anyone experienced such situations during their life. But not at this frequency. To counter this intensive VUCA time we must reassess quicker our posture and take inspiration from the Agile software development principle: you treat Volatility with strategic Vision. You approach Uncertainty with Understanding. You crunch Complexity with Clarity. You react to Ambiguity with Agility.

Fast adaptation must not equate short-sighting. See far, act near. It is even more important to develop a strong long-term vision. We just need to set more frequent checkpoints on the way to our objectives to perceive and act on changes quicker.

Achieving Cyber Resilience

Cyber Resilience is the path where a successful cyber intrusion have little impact on you or your organization. You are back on your feet quickly and ready to dodge the next shot:

- Hygiene: infuse basic hygiene in your organization that create the minimal security baseline
- Strategy: engage top executive ready to lead the fight back
- Assess: create a map of your riskier operations and focus your effort on them
- Measure: make rough quantification to prioritize where you start improving
- Mitigate: fix and monitor the weakest points
- Train: employee training, security drills and crisis simulation help stress-test the organization, develop skills and sharpen awareness
- Capitalize: analyze what you did well, what could be improved and what must be reviewed.

Finally, start again: by increasing hygiene and reducing one by one the weakest points you adopt a continuous and dynamic improvement posture enhancing your security readiness.

PREPARATION IS KEY

Cyber-Resilience is the ability to recover faster, with minimal cost, to a cyber-attack. It involves careful planning and strategy. Prevention minimize likelihood and impact; resilience optimize the impact reduction. But the later cannot be achieve without strategic preparation and risk prevention.

XRATOR
CONQUER YOUR RISK

Protect your business

Talk to your local expert
Gert Van de Ven
VP Sales, ASEAN
gert@x-rator.com