Computacenter

# NEW YEAR. NEW SECURITY RESOLUTION.

## Security White Paper

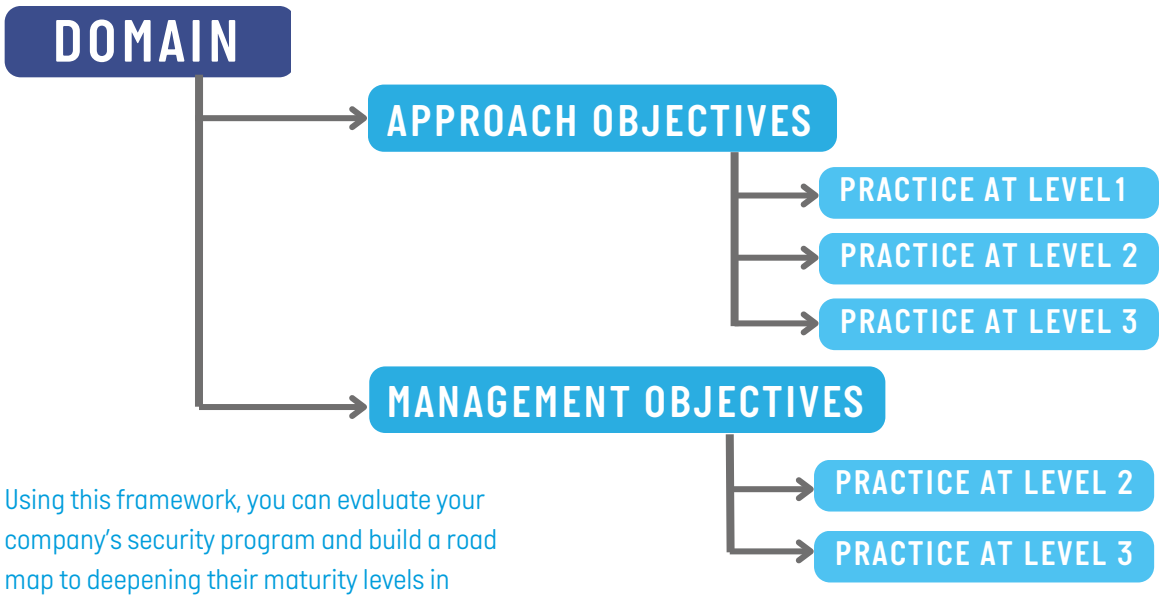
# NEW YEAR. NEW RESOLUTIONS.

With last year behind us, we look forward to a new year and with that comes new year's resolutions. However, have you thought beyond your personal resolutions? What about setting some organizational goals as well, such as reducing cybersecurity vulnerabilities, implementing threat procedures, or leveraging training to decrease security slip ups.

Bruce Schneier once said, "security is a process, not a product"[1]. Despite this, today's market tends to talk about security as one product, you either have it or you don't. However, in reality security is multiple processes working in tandem to support your business.

The Cybersecurity Capability Maturity Model (C2M2)[2] is a security process framework that focuses on the implementation and management of cybersecurity practices associated with information technology (IT), and operations technology (OT) assets and the environments in which they operate. Using this approach, we can quickly evaluate a variety of cybersecurity practices grouped by domain, allowing organizations to focus on implementing practices to improve their maturity in a domain.

## SIMPLIFIED C2M2 FRAMEWORK




Using this framework, you can evaluate your company's security program and build a road map to deepening their maturity levels in different domains.

1 HTTPS://WWW.SCHNEIER.COM/ESSAYS/ARCHIVES/2000/04/THE_PROCESS_OF_SECUR.HTML
2 HTTPS://WWW.ENERGY.GOV/CESER/CYBERSECURITY-CAPABILITY-MATURITY-MODEL-C2M2

**CLICK TO READ OUR CYBER SECURITY WHITE PAPER**

Evaluating which domain to focus on can be a challenge with the many competing priorities. While Risk management can play an integral role in your security infrastructure (read the 5 Questions You Should Be Asking About Your Cyber Security white paper to learn more), vulnerability management has several compelling reasons why it is a great domain to tackle first:

1. It's complementary to risk management.

2. It can be very difficult. Market experience shows a multitude of security assessments where out of date and unpatched software are by far the biggest issue.

3. It's essential that most organizations, even those doing the bare minimum, have implemented at least some vulnerability management habits.

The overall objective of Vulnerability Management is to establish and maintain technology, processes, and people in order to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities to organization computing, network, and data.
There are three overarching objectives:

1. Reduce Cybersecurity Vulnerabilities – This begins with collecting and analyzing vulnerability information through vulnerability discovery. Following this a vulnerability analysis should identify the vulnerability's impact, i.e. the potential effect of the vulnerability on the asset, as well as the importance of the asset to the proper functioning of the business.

2. Respond to Threats and Share Threat Information – This may be addressed by implementing mitigating controls, monitoring threat status, applying patches, applying hardened configuration, and replacing outdated equipment. This information may be shared with stakeholders internally or externally.

3. Management Activities – Ensures procedures are documented, followed, and maintained. Resources are provided to make sure that tools are available, and that people are trained to use those tools effectively.

Each of these objectives can be done well or poorly. This is measured by the maturity level.

MATURITY LEVEL 1:
Some rudimentary practices are performed, but they tend to be done in an ad hoc fashion.

MATURITY LEVEL 2:
Habits and practices are performed on a regular schedule and/or according to defined triggers. Operational impacts are considered prior to fixes being applied. Information is shared with stakeholders. Habits and practices in this domain start to interact with other domains.

MATURITY LEVEL 3:
Assessments, penetration test, and audits, are performed by organizations (internal or external) that are independent of the operation function. The vulnerability management domain starts to provide input to, and take output from, the risk management domain.

# AN EXAMPLE:

Hypothetical Company A has the following vulnerability management program in place:

HYPOTHETICAL COMPANY A

- They have a vulnerability assessment tool such as Tenable Nessus, Qualys, Rapid7, or OpenVAS.
- They periodically run the tool, but it's done in an "out of the box" fashion and only occasionally.
- The reports from the scan are reviewed but only some of the critical findings are addressed.
- Once a year, or longer, they have an outside company perform a "black box" penetration test. Those results are reviewed and shared with the senior IT team.
- As part of their PCI Compliance program, they have their external web servers scanned once a quarter.
- Company A has a policy about vulnerability scanning and penetration testing, but it hasn't been reviewed or updated in over a year.

This barebones program would barely rank at a maturity level 1, things are done in an ad hoc manner, there is no regularity to the scanning, the tools suite only provides minimal coverage of information assets, they haven't optimized the tools that they do use, and the results don't make it very far up the reporting chain and are definitely not being incorporated into their risk management framework.

What could Company A do, starting tomorrow, in order to immediately improve their maturity in vulnerability management? Just like New Years resolutions it may be tempted to think big and try to do too much too soon. However, creating realistic small steps that can be built upon is key to successfully reaching your goal. Small steps could include:

- Make a list of all the technology that you use and that you are going to include in the program at the moment (it should expand as you get better and buy more tools).
- Pick a schedule to run your vulnerability scans on. At the very least it should be quarterly, better would be monthly to coincide with typical patching cycles. Include the schedule scan in your regular change process so everyone knows it will be happening and when.
- Your tools don't know what is important to your business (at least not out of the box). Review and interpret the results according to impact to business criticality.
- Arrange a regular meeting, that aligns with the regular scanning schedule, with stakeholders outside of IT operations to discuss the results, discuss mitigations, and prioritize fixes.
- Incorporate this information into regular change review processes, and your IT risk management process.

These simple changes can be the first steps towards developing your vulnerability management to maturity level 1. Level 2 will build upon this foundation. and requires better use of tools, and a variety of them along with better training of resources and functioning domains. It requires better use of tools, possibly a wider variety of them, along with better training of staff in their use.

We only discussed one of the many habits you have to have for a well-rounded security program. If you'd like us to review your program we can take you through our Cyber Security Lens to provide you a high-level overview of your security stance. We'd like to work with your organization to help achieve your New Year's security goals.

# WHO WE ARE

## COMPUTACENTER

Computacenter TeraMach, Inc. (CC TeraMach) has over 24 years of experience in the public sector, education, healthcare, and commercial industries, focusing on Digital Transformation in the areas of Security, Cloud, and Edge. Our extensive data centre technologies' experience, digital services capabilities, strong vendor relationships, and deep technical knowledge has enabled us to be the trusted partner for our 2000+ satisfied customers.

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. Together, we help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling people and their business.

# WHO YOU'LL CONTACT

## JASON MURRAY
### SOLUTION ARCHITECT AND TRUSTED ADVISOR

### PROFILE

Jason is based out of Toronto and is passionate about solving security issues within the Educational space.

### EXPERIENCE

With more than 20 years of experience in the technology sector Jason has the technical skills to support your business in achieving their digital transformation goals.

**Our team of IT experts can help answer your most pressing cyber security questions, give your organization peace of mind with cyber security services from Computacenter.**

**Connect with our cyber security experts today +1 (647) 333-6241**