



Take Control With Cybersecurity

Value, Workflow And Peace Of Mind
In An Ever-Digitalizing World

CGI

An Introduction To Cybersecurity

The business world is developing rapidly in our digital age. It seems like the possibilities are almost limitless. Digitalization redefines value chains everywhere—connecting both people and machines globally. AI, networking, machine learning, social media, automation, virtual reality and industrial internet are the magic words on everyone's lips and appear in almost every company's strategies.

But connecting these dynamic needs necessitates vigilance against cybersecurity threats. You may ask your-

self, am I gaining or losing value? How do I protect my personal information? Is my business safe? What should I do? These indeed are the most important questions you can ask yourself. Nothing replaces the importance of being well prepared.

At CGI, we focus on providing services via the positive, rather than utilizing scare-tactics. Our business is all about your value, workflow and peace of mind. This is why the CGI Cybersecurity Center was established: to help you take back control.



Sincerely Yours,

Jan Mickos

Vice President, Cybersecurity at CGI

Table Of Contents



| | |
|---|-----------|
| The Control Is Yours..... | 4 |
| The Big Why..... | 6 |
| The Root Causes..... | 7 |
| Prepare Yourselves..... | 8 |
| What's Next..... | 10 |
| Your Steps Into Security..... | 11 |
| CGI Cybersecurity Centers At Your Service..... | 12 |

“Nothing replaces the importance of being well prepared.”

– JAN MICKOS

The Control Is Yours

Currently, cyber-attacks are considered to be one of the biggest threats in the business world. Globally an average company experiences several cyber-attacks every month—either knowingly or unknowingly. There is a real possibility that yours is one of them. Many of these attacks happen without anyone noticing them, or by the time they are in the headlines. At CGI, we are committed to help you to accomplish more than just security.

First, what has cybersecurity to do with your business value? A lot. Many businesses have lost their entire market value just by leaking their valuable data. We won't name any examples, but we are sure you can find them. But on the other hand, more businesses have gained value by properly protecting themselves. Actually, cybersecurity is one of the most valuable market differentiators right now.

Second, cybersecurity has everything to do with your workflow. When individuals learn why they should care about their personal security, they'll apply this awareness into practice in their daily work. In reality, it's the people that make your business run smoothly and without slowing it down.

Third, the most important thing is your peace of mind. Realizing such threats exist, there is no need to panic. The biggest mistakes are often made when people begin to panic and rush with their own solutions. To prevent stress caused by threats, our global and unique Situation Awareness Services empowers you to stay one step ahead.

We are committed to turning your security problems into possibilities. With CGI, the control is yours, 24/7/365.



LOW

30

The Big Why – Why Your Data Is So Precious

Think about this: our society and businesses run on data. It fuels the whole system. What if your customer's, employer's or product information would leak? What if outsiders could control your hardware? How could this harm your brand? What would happen to your cash flow? Or to your community? The most crucial realization is that you are actually making your money with data, no matter which business sector you are in. That means the value of your data equals your company value.

”That means the value of your data equals your company value.”

The Bright Side

As a Business Owner, you will benefit from the added security in many ways. First of all, your brand becomes more valuable, and you become a genuinely trusted partner. Your employees and customers will be more satisfied, happier and committed. At the same time, all the business operations can continue without expensive distractions. Your investors will tap you on the back as you walk into your office.

For ICT personnel and those responsible for your company's Security, added cybersecurity means finding the right methods and seeing your operations as an important investment. Not only will you sleep better, but lead better. Your team will be more proactive instead of merely reactive.

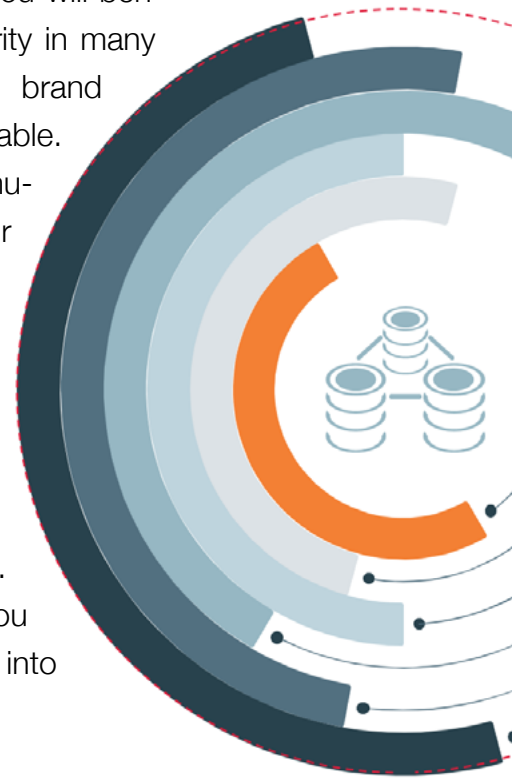
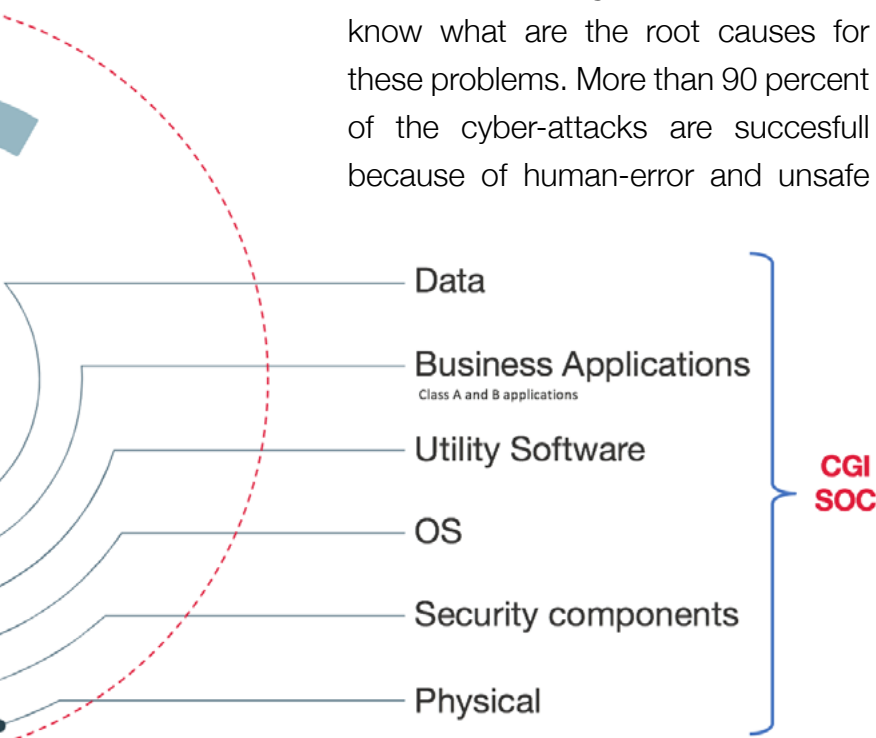


Image:
Application Aware

The Root Causes – How the Attacks Are Designed And Take Place

Every year hundreds of millions of euros are spent on cybersecurity. However, you might be surprised to know what are the root causes for these problems. More than 90 percent of the cyber-attacks are successful because of human-error and unsafe

daily operations and unsafe working methods. It's also common to become a victim of social engineering. What is social engineering, you may ask. Social engineering refers to confidence tricks, psychological manipulation of people into performing certain actions or disclosing confidential information. And a surprising percent of this is actually perpetrated by so called company insiders, trusted people with remote or physical access to your company's assets.



Security Operations

operations. The cyber-attacks are designed in such a way as to make the best use of these weaknesses. Nevertheless, approximately 10 percent of the attacks will succeed regardless.

Unintentional damage stems from various reasons, including lack of appropriate personal awareness, unsecure

At CGI, we operate on every level of cybersecurity, including application monitoring and secure programming. When the attackers get real authentications, they rarely get caught. This is where application monitoring does the trick by recording who is using your data and how. We are also familiar with targeted malware attacks, advanced persistent threats and commodity malware hacking (for example attacks by showing infected advertising banners).

Prepare Yourself – Calm Is The New Super Power

As our client, you are never left alone with cybersecurity issues. CGI provides the people, tools and processes to protect your digital business. We do this by assessing the risks and helping you develop secure digital services, while continuously monitoring and protecting against existing and emerging cybersecurity threats on a daily basis. You'll feel secure and in control as CGI continuously maintains your security status, which means that you'll get a holistic and an up-to-date understanding of the situation.

We will move you from a compliance-driven approach to a risk-driven approach – build a proactive capability status based on a specific risk profile and not on a generic set of compliance standards.

Our Cybersecurity Centers continuously monitor your ICT environment. We help you take control by monitoring and analyzing your event stream in accordance with the current global threat landscape. When a suspected threat is found, we first eliminate the false alarms, and when the threat is real, we immediately take care of it and prepare for the next possible threat.

The Steps For Gaining Control:

| IDENTIFY | PREVENT | DETECT | REACT |
|--|---|---|---|
| Develop the organizational understanding in order to manage cybersecurity risk to systems, assets, data, and capabilities. | Develop and implement the appropriate safeguards to ensure safe operations of the business. | Develop and implement the appropriate capabilities to identify the occurrence of a harmful cybersecurity event. | Develop and implement the appropriate activities to take action in dealing with a detected cybersecurity event. |



What's Next? – Taking Your Security To The Next Level

Security threats do not respect geographical boundaries. Therefore, monitoring must be in place in every corner of the world to protect a business in a genuinely proactive way. Through our global network of Security Operations Centers (SOCs), we have a 360-degree view of threats across sectors and different geographical locations. Our security services teams continuously identify and deploy advanced solutions to maintain a state-of-the-art infrastructure.

Our global experience helps us predict and defend against new attacks, and our front-line capabilities reflect this knowledge.

We collect Threat Intelligence from a wide range of sources:

- Open Source Threat Feeds
- Partner and Vendor Threat Feeds
- Commercial Threat Feeds
- National Authorities Threat Feeds
- CGI Internal Threat Feeds

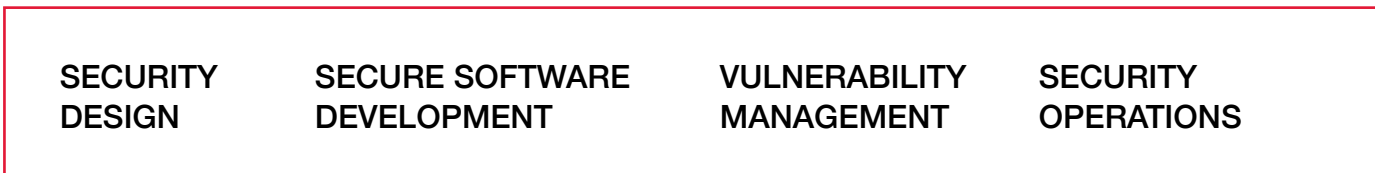
Our 24/7/365 Service Also Includes:

- Advanced Detection Capabilities, including Artificial Intelligence and Machine Learning
- Advanced Network and End-point Protection
- Managing and Operating Technical Controls
- Threat Intelligence driven Custom Fingerprints for Sensors
- Vulnerability Management and Analysis
- Forensics and Threat Hunting



Your Steps Into Security

Security Lifecycle Process



“As our client, you are never left alone with cybersecurity issues.”

– JAN MICKOS

Assess The Risk. Protect Your Business. Operate With Confidence.

– CGI Cybersecurity Centers At Your Service

At CGI, security is part of everything we do. We take a business-focused approach at every level—from threat and risk management to response and recovery. Our comprehensive services include consulting and training, integration and implementation, managed services and security operations. We offer you both global and local power, as well as a genuinely close and holistic ICT approach.

CGI – Control With Cybersecurity:



9+/10 Customer Satisfaction



Motivated and Satisfied staff at your service



35+ years of experience in information security across government and commercial sectors



3 accredited test facilities Canada, US and UK.



1500 cyber professionals globally, 250+ in Northern Europe.



7 Security Operations Centers globally, 1 in Finland



Versatile, non-dependent of a specific technology, delivery, service-model or operations.



Tested and proven in some of the world's most sensitive and complex environments



We are the only full-service cyber security provider

Contact

Mika Heino

Director, Security Operations Center, CGI
Tel. +358 40 777 0370
mika.heino@cgi.com

Jan Mickos

Vice President, Cybersecurity, CGI
Tel +358 40 847 8740
jan.mickos@cgi.com

www.cgi.fi/kyber
www.cgi.com/cyber

CGI