C*

*CYBERSECURITY 18

CGI

IT security is a top priority for Alecta

Saving energy and lives

Valmet is taking care of the basics

Identifying the risks

Building secure outcomes

Operating with confidence

WELCOME HACKERS

MÅRTEN MICKOS

Editorial

Face the reality

CYBERSECURITY today is on the critical path for digital organisations as a business issue.

Modern security risks require efficient monitoring which takes advantage of technology and human expertise. The reality is that organisations still tend to rely on technical solutions. Another common problem is an unrealistic trust in the ability to avoid and detect cyber incidents.

Surprisingly often, information about discovered breaches are passed on from outside the organisation – from customers, the authorities, or hackers.

For this issue we collected stories and examples to help you get a handle on the risks, build secure outcomes and operate with confidence. Have a cybersecure rest of the year!

Heikki Nikku
President, CGI Northern Europe

CGI

CGI is among the largest independent IT and business consulting services firms in the world. With 74,000 professionals across the globe, CGI delivers an end-to-end portfolio of capabilities, from IT and business consulting to systems integration, outsourcing services and intellectual property solutions. This is CGI's Cybersecurity themed client magazine published in the Northern Europe countries. Learn more at cgi.dk, cgi.ee, cgi.fi, cgi.com/norway, cgi.com/polska, cgi.se.

Editor in Chief Jarkko Virtanen, jarkko.virtanen@cgi.com,
Managing Editor Esa Luoto, esa.luoto@cgi.com,
Edited and published in cooperation with Legendium Oy.
AD Laura Ylikahri. **Cover photo** Jussi Nukari / Lehtikuva
ISSN-L 1455-1934, ISSN 1455-1934 (printed), ISSN 2323-153X (online)

There is no such thing as zero cyber risk. We should therefore focus on minimising, rather than eliminating, the risk.

Read the inteview of Mårten Mickos at page 9

PHOTO BUBBERS BB / SHUTTERSTOCK.COM

SEVEN FATAL CYBER SINS

Ensuring the Cybersecurity of a company is affected by several human factors.

TEXT JAN MICKOS

1. DENIAL

- Companies have a firm belief in their staff's ability to defend themselves against cyber criminals. Up to three out of four organisations* believe that they are able to detect cyber-attacks themselves.
- **THE MORAL OF THE STORY:** Recognise actual threats. Even if you were protected yesterday, it is not enough today.

2. DEFICIENT MANAGEMENT

- A large proportion of companies rely on network-level monitoring, even though only 40% of malware is caught by anti-virus software and firewalls.
- **THE MORAL OF THE STORY:** Appoint a senior executive to be responsible for information security. Information security requires strategic management.

3. INSUFFICIENT RISK MANAGEMENT

- Cyber attackers typically find the weakest link in the value chain and then target the most valuable operator. The value of a listed company can decrease by as much as 15% due to a serious data breach.**
- **THE MORAL OF THE STORY:** Cybersecurity is a business risk. You should require that service providers comply with your information security requirements.

4. POOR CYBER HYGIENE

- Poor cyber hygiene, i.e. inadequate management of the bare essentials, is the cause for 83% of Cybersecurity incidents.
- **THE MORAL OF THE STORY:** Cybersecurity culture requires persevering work. Train your employees, practice and test. Define information security resources that match your objectives and obtain support from a partner who helps you choose technologies and provides consultation and training.

5. TECHNOLOGY AGNOSTICISM

- The fast technological development can make one believe that a solution for Cybersecurity challenges will soon be available. In reality, cybersecurity risks cannot be controlled merely with technology.
- **THE MORAL OF THE STORY:** Security risks require intelligent technology, relevant threat intelligence and human expertise – True Intelligence.

6. POOR ABILITY TO RESPOND

- Despite precautionary measures, approximately 10% of attacks are successful. If you are the target of a cyber-attack how fast can you get the situation under control?
- **THE MORAL OF THE STORY:** Ensure operational ability in all situations. Train, practice and test. Make a contingency plan and establish an incident response team.

7. FORGETTING CONTINUOUS DEVELOPMENT

- Cybersecurity is not a single project.
- **THE MORAL OF THE STORY:** Identify development needs, create a roadmap and a plan for continuous monitoring, measurement and development. Remember to monitor cybersecurity in the value chain as well.

*The status of cybersecurity in Finnish organisations in 2018, research by CGI Finland
** The Cyber-Value Connection survey, CGI UK

Read more in your own language at cgi.dk, cgi.ee, cgi.fi, cgi.com/norway, cgi.com/polska and cgi.se.

IN REAL LIFE, BORING IS SAFE – ALSO IN CYBERSECURITY

IN CYBERSECURITY, The vast majority, 83%, of incidents are cases of bad security hygiene: unpatched systems with default passwords get infected with malware because the user clicked on something. 99 % chance is you do not need a SOC to fight your nation-state cyber adversaries. You need it to remind you to brush your teeth and wash your hands after flushing. You need a SOC and its brilliant minds of highly skilled cybersecurity professionals to make sure you bother to do something about your security hygiene. * JAN MICKOS

WILL AI RESOLVE YOUR CYBERSECURITY PROBLEMS?

LOOKING AT all the buzz around these emerging technologies, one could think that technology will resolve all cybersecurity problems. In reality, technology alone cannot make a difference in cybersecurity.

To defend against existing and emerging cybersecurity threats, organisations need a seamless combination of intelligent technologies, threat intelligence, and the intelligence of brilliant minds of highly-skilled cybersecurity professionals – "True Intelligence". * JAN MICKOS

WITHOUT TRUST THERE IS NOTHING

ALL THROUGH human history, fraudsters have pretended to be who they are not in order to trick people out of their possessions. In order to prevent this online, there is a need for a solution, which guarantees that the person you are dealing with is who she says she is. It all comes down to trust. Trust from a customer buying something from you, trust in the eshop selling something to you, trust in that the data you have been sent for decision is the correct one. * GUNNAR KLINTBERG

SOC
DEFENDS AGAINST CYBER THREATS

"Only 6% of organisations are sufficiently capable of protecting themselves against attacks."

TEXT ESA LUOTO PHOTOS ANTTI KIRVES GRAPH LAURA YLIKAHRI

Cyber attacks are hitting the news on a daily basis. Nevertheless, many companies and organisations are not adequately prepared to combat them. CGI's **Jan Mickos**, Vice President, Cybersecurity, provides an example.

"As many as 94% of organisations affected by cyber-attacks will become aware of it from a third party. Only 6% of organisations are sufficiently capable of detecting evolving threats themselves."

Jan Mickos emphasises that traditional anti-virus and network firewalls, or even competent personnel, are no longer enough to prevent against modern threats. Cross correlating the various events in the cyber environment to form a coherent and up-to-date view of the situation and the extent to which this situational awareness can be used to identify and respond to complex adverse events have become a necessity and a challenge.

360-degree visibility to cyber threats

In Finland, CGI is the only supplier with total solutions for cybersecurity. A key part of CGI's cybersecurity services is provided from Cyber Security Operations Centers (SOCs). In addition to the SOC in Finland, the company has seven SOC units around the world. This network enables CGI to have an extensive and global understanding of the threat landscape.

Jan Mickos

"For our customers, this provides an opportunity for more proactive and comprehensive situational awareness and better cybersecurity. The international network of SOCs monitors and protects the partners' cybersecurity around the clock and across borders. We provide a 360-degree visibility over cybersecurity threats in relation to both technology and business. We monitor global cyber threats, filter false alarms and, when it comes to the crunch, we take the reins, prepare for the next attack and carry out forensic investigation," says Mickos.

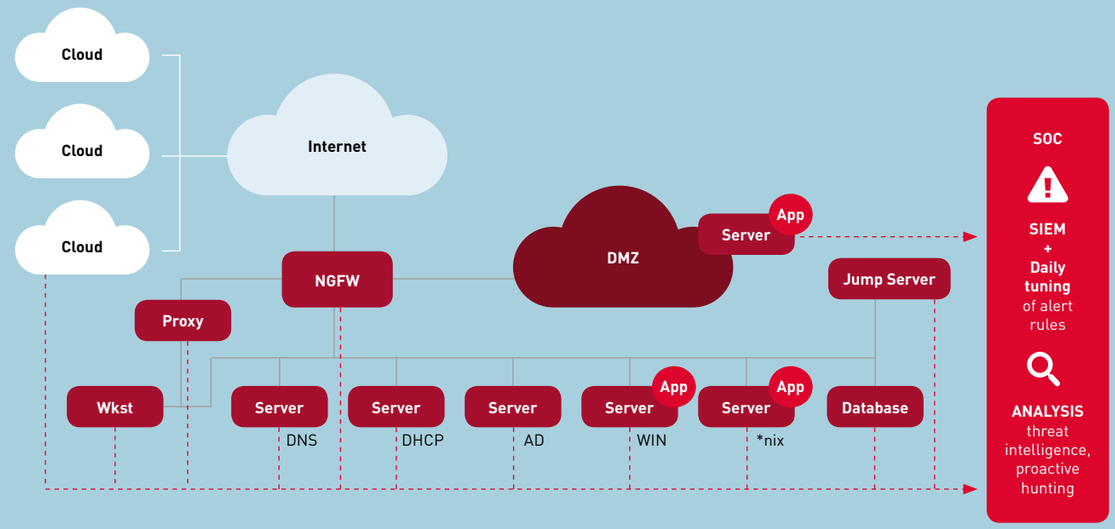
In the future, CGI's Cyber Security Operations Center in Finland will be providing continuous information security monitoring to its customers in other North European countries as well. *

EXAMPLES OF THE SERVICES PROVIDED BY CGI CYBER SECURITY CENTER

Continuous cybersecurity services:
- Continuous security monitoring
- Continuous security monitoring for business applications
- Security incident response
- Digital forensics and proactive threat hunting
- Continuous management of vulnerabilities

Consulting services for cybersecurity:
- Health checks
- Penetration testing and Red Team drills
- Information Security Manager services and development of security management and control
- Cybersecurity development projects

WOULD YOU LIKE TO ASK SOMETHING?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com



In addition to the Security Operations Center in Finland, CGI has seven other centers across the globe. This global network of SOCs provides a uniquely broad and comprehensive view on both existing and emerging cybersecuity threats, both globally and locally.

TEXT SAMI LAAKSO PHOTOS HACKERONE AND SHUTTERSTOCK

Cyber risk is never zero percent.
Within companies, the key issue is to minimise such risks.

CYBERSECURITY FROM WHITE HATS AND RECOGNITION OF FACTS

The NotPetya cyber attack caused a loss of EUR 240 million for Maersk, the Facebook data leak put more than 50 million user IDs at risk, the Ministry for Foreign Affairs has been subject to cyber-espionage, there have been disruptions of online banking, and online users have received extortion messages...

There has been no shortage of news about cyber crime, even if a large number of cases remain hidden from the public. **Mårten Mickos** is convinced that more such news is on the way. The worst is yet to come.

"Cyber attacks will become even more serious than they are now. But solutions and countermeasures have also begun," he says.

Mårten Mickos has a clear perspective of these issues. He is the CEO of HackerOne, which is based in Silicon Valley. His career includes an impressive line-up of workplaces and businesses, including MySQL, Sun Microsystems, Eucalyptus Systems and Hewlett-Packard.

WHO?
Mårten Mickos

WORK
CEO of HackerOne

CAREER
Leadership positions in several technology companies, such as MySQL, Sun Microsystems, Eucalyptus Systems and Hewlett-Packard

EDUCATION
Master of Science (Technology)

Concrete action is needed now

There is an alarmingly wide spectrum of cyber threats, as headline cases have brutally revealed. The sky is the limit to the dark scenarios that can be imagined.

"There are many cyber threats and it is impossible to judge which would be worst. It's terrible if your credit card or bank credentials are stolen. But it would be worse if the information systems that drive society went dark. It would be even worse if the power supply or healthcare came to a halt. There may be even more horrific scenarios, with very expensive consequences," Mickos speculates.

Mickos believes that, at worst, a cyber attack could undermine the public's faith in society.

"The result could be chaos and a breakdown in the social order," Mickos comments.

Despite these gloomy notions, he points out that the worst scenarios are not inevitable. Much depends on our ability to defend ourselves and proactively improve the situation.

HACKERS-AS-A-SERVICE

FINNISH COMPANIES will be the first in the world to have access to the competence of a global hacker network combined with CGI's cyber security expertise.

"Hundreds of security vulnerabilities can be found per day with help from the global white hat hacker community. Assessing vulnerabilities in terms of its relevance and urgency is vital to a programs´ success. This requires expertise and resources, and as Finland's largest and as a global provider of these specialist services we will now also cover these bounty programs," says **Jan Mickos,** CGI Finland's Vice-President for Cybersecurity.

Members of the network will look for security vulnerabilities in the system or application that is to be assessed without any special access required. If vulnerabilities are detected, the hackers receive recognition. The form and the size of the reward varies depending on the gravity of the vulnerability or the program scope.

"Bug bounty programs are a proven way to find where companies and organisations are most vulnerable by using similar security testing techniques as the hackers use," says Mickos. CGI will use Hackers-As-A-Service concept in offering vulnerability analyses and it's end-to-end cyber security services.

"Luckily, society and various players within it have already recognised these risks and taken countermeasures. The most advanced organisations view security as a risk management activity. Many people understand that defenders should share information and cooperate with one another. The value of third-party vulnerability reports is recognised. It is now just a question of how fast – or slowly – the ship can be turned around," says Mickos.

And there is a lot of turning to be done on the ship – or actually the many ships. Since people are often the weak link in cyber security, awareness and measures taken at organisational level are not enough. A careless user can open the door to scammers.

Mickos emphasises that cyber security problems are so widespread and significant that everyone should be aware of them.

"Everyone can reduce the risk of cyber attacks by exercising caution and discipline when using computers. Take backups. Do not open attachments or click on links in emails," says Mickos, reminding us of the basics.

Welcome hackers

So what tactics should be used to counter cyber threats? "Of course, perfect security from cyber threats would be the best option," says Mickos, "calling for realism." He believes that cyber defence is not about seeking a technology that would stop all attacks, but minimising the risks.

"We should acknowledge that there is no such thing as zero cyber risk. We should therefore focus on minimising, rather than eliminating, the risk. This would have major results and tolerable costs."

This risk-reduction philosophy is also being implemented by the company led by Mårten, HackerOne, which has a network of around 250,000 so-called 'white hats.'

These white hats are hackers who use their talents responsibly to promote cyber security and trust. In many cases, they receive a 'bounty' for discovering vulnerabilities in the system or application they are hacking.

For companies and organisations, the cooperation involves taking action in advance to identify software and application vulnerabilities, by using similar methods to those used by cyber criminals.

"The risk of data intrusions decreases when a company fixes an identified bug. It has been noted that this is a more effective and cost-effective way of seeking and identifying security vulnerabilities than all other approaches," says Mickos, listing the benefits.

As many as hundreds of vulnerability reports per day can be generated by a white hats network, through so-called Bug Bounty programmes. The importance and urgency of each vulnerability must be assessed.

"This involves expert work that requires resources and knowledge. Few companies have enough of these. But for this work, you can – and in general you should – turn to a specialised partner for the analysis and management of vulnerabilities," states Mickos.

We should acknowledge that there is no such thing as zero cyber risk. We should therefore focus on minimising, rather than eliminating, the risk.

3

tips on how to minimize the risk of a cyber breach

1. **Minimize the risk, since eliminating the attacks is not realistic.**
2. **Prepare in advance and assess the level of your security with white hat hackers.**
3. **Human is typically the weakest link. Rise the cyber-security awareness and skills of your employees.**

WOULD YOU LIKE TO ASK SOMETHING?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com

Not everyone has woken up

So what is the situation in Finland? According to CGI's survey, in the last two years, every fifth organisation has already been the subject of extortion malware, and every third of other types of malware. Only 13% of organisations inform the public of the occurrence of cyber attacks or damage. Up to 70% of organisations estimate that they are likely to be attacked sometime during the next year.

Mårten Mickos believes that there are two sides to the situation.

"Finland, on the one hand, has the world's best security expertise, but there is also widespread denial of the problem."

Mickos encourages organisations to make security a core priority. This means that, in addition to security-based application development, systems must be subject to continuous data security measures, and organisations must be prepared for possible attacks and other incidents.

He explains that modern players also understand the importance of transparency. The potential for cyber risk reduction can be increased many times by sharing information and listening to external experts.

Although cyber threats may seem daunting, Mickos points out that the cyber risk scenario is no worse than that of any other significant threat.

"We must see and acknowledge the facts. We should start taking corrective measures. We must not believe in total security. It is about the conscious and systematic management of risks," he sums up. ✱

ABOUT ALECTA

ALECTA LOOKS AFTER occupational pensions for 2.4 million people and 34,000 companies in Sweden. The company is owned by the customers and only handles collectively agreed occupational pensions such as ITP. Alecta is one of the biggest owners of the Stockholm Stock Exchange and one of Sweden's biggest property owners. The company was formed in 1917 and currently has around 350 employees.

ABOUT SOC

CGI'S GLOBAL NETWORK of Security Operations Centers (SOC) provides a total overview of various threats across all sectors and geographical locations. CGI's security teams identify and deploy advanced solutions continuously in order to maintain infrastructures. CGI has close collaboration with international security organisations and standardisation bodies, and is one of the few suppliers to have three officially approved facilities for security certification– in Canada, the UK and the USA, including the world-class CGI Federal Cyber Innovation Lab.

IT SECURITY
IS A TOP PRIORITY FOR ALECTA

The trust of its customers means everything to pensions giant Alecta. This is why the ability to protect their customers' information is one of the most important parts of the business. Together with CGI, Alecta has reinforced its cybersecurity dramatically in recent years. At the same time they have created ways of working more proactively to deal with current threats.

TEXT MATTIAS KARÉN PHOTOS EVELINA CARBORN AND SHUTTERSTOCK

With almost 2.5 million private customers, Alecta is Sweden's biggest occupational pension company. Alecta manages more than SEK 800 billion in capital, an enormous responsibility that also demands IT security of the very highest level.

"In our industry, credibility is extremely important. The customer must be able to rely on us to manage their information in a safe, responsible way. That's our top priority. We can't afford to lose that trust," says **Ulf Larsson,** Head of IT at Alecta.

To secure its customers' information and funds, Alecta has chosen to outsource IT operations to CGI. This collaboration started back in 1996 and was reinforced considerably over the last five years as cyber security moved higher up the management agenda.

> ***In our industry, credibility is extremely important.***
>
> **ULF LARSSON**
> Head of IT, Alecta

"We've increased investments significantly in just a few years when it comes to IT security, and together with CGI we've increased the levels of protection. IT security is now part of virtually all commercial businesses and an issue that is dealt with at Board level. That's not how it was five, ten years ago. There's a very big difference," says Ulf Larsson.

Among other things, Alecta made a strategic decision to follow the international standard ISO 27 000 for IT security. They are also using CGI's security service SOC (Security Operations Centers) to maintain a total overview of various threats.

3 tips on IT security

1. Don't think you can do it all yourself. It's a large, complex area that is constantly growing. You must ally yourselves with experts and build up extensive collaboration with them.

2. Set a clear standard that you work by, that helps all employees to focus on meeting that standard. If you can't agree on which way you're heading, all initiatives will be left hanging in the air.

3. Make sure that the whole management team is on board and has a focus on this area. If it's not already on the Board's agenda, it must be. Otherwise you have to fight for every initiative. There must be an awareness at management level that this is important.

At Alecta, IT security is now part of virtually all commercial businesses and an issue that is dealt with at Board level.

"The biggest threat is that you don't take this seriously. So it feels extremely reassuring to have such a big and competent partner as CGI, who take our security very seriously indeed. Because we're good at developing insurance systems, but we're not as good at IT security," says Ulf Larsson.

Like all major financial companies, Alecta has to protect itself against both internal and external threats. They also have to deal with continuous internal audits as well as inspections by the Swedish Financial Supervisory Authority and other bodies.

"After all, there's a lot of money passing through our systems, so we have to be protected from both a system perspective, and do the right thing internally. For us, it's a question of reassurance that we're doing the right things. Then something can always happen even so. But we've worked seriously and credibly on these issues and can be certain that we're at a good level," says Ulf Larsson.

Services such as SOC also help Alecta to protect itself against new global threats, and Ulf Larsson believes that these kinds of proactive solutions are an important strategy to deal with a future in which more and more of the IT infrastructure is in the cloud.

"SOC is helping us to take the step from reactive IT security to proactivity, and shows that CGI has in-depth expertise that we can never achieve ourselves in this area. Security nowadays is largely about proactive monitoring and pattern recognition and the likes. We must be on board that train," says Ulf Larsson. ✱

Q&A

Information security is worth protecting

When cyber risks materialise, they could threaten the entire existence of the company. A cyber insurance policy aimed at SMEs provides cover in the event of cyber damage.

1 WHAT ARE THE MOST TYPICAL CHALLENGES THAT COMPANIES FACE IN THIS AREA?

Especially smaller companies have challenges with recognising cyber risks related to their business and operational network. It may also be difficult to understand how various digital solutions are linked to the company's business and how they affect its financial results. In addition, the new General Data Protection Regulation, its requirements and implementation may be a challenge.

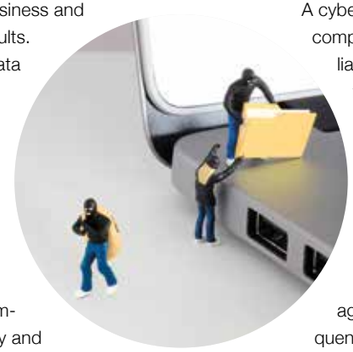
2 HOW SHOULD I PREPARE FOR INFORMATION SECURITY RISKS?

An information security policy or instructions describing the importance of information security and data protection to the company's business should be prepared, and all employees should receive compliance training. Regarding information security, the minimum requirement is to protect the company's ICT devices and networks with up-to-date anti-virus software, firewalls, and backups.

3 WHY SHOULD I OBTAIN A CYBER INSURANCE POLICY?

In the worst case, a cyber-attack can interrupt the company's business for a long time and cause significant financial losses to the company, its partners and customers. Traditional insurance policies do not cover the cost of security breaches, data loss or costs incurred as a result of other similar cyber risks. Information owned by another party, such as customer data, is often at risk. Data may be lost or fall into the wrong hands.

A cyber insurance policy enables the company to partially prepare for the liabilities and obligations they are facing after a cyber-attack or a security breach.



4 WHAT DOES THE CYBER INSURANCE POLICY COVER?

It covers direct crisis management costs up to the agreed insured amount, consequential losses incurred by the policyholder and financial damage incurred by the other party as a result of the security breach. Crisis management costs include the costs of expert services. It also compensates for the costs of restoring files and software and the costs incurred as a result of the communication obligations set out in the General Data Protection Regulation.

The cyber insurance will not compensate for personal injury, suffering, property damage or fines. In addition, the insurance will not cover damages incurred as a result of inadequate firewalls or anti-virus software or the failure to take daily backups.

Sami Kehusmaa
Team Manager, OP

Take care of THE BASICS

Sakari Koikkalainen, IT Security Manager with Valmet's IT infraservices, points out that risk-based cybersecurity helps to secure the basics of data security cost-effectively.

TEXT ARI RYTSY PHOTOS KRISTIINA KONTONIEMI AND SHUTTERSTOCK

"Environments previously unconnected with information technology are now connected and will continue to be in the future. This is creating new business risks in areas such as cybersecurity. It means that cybersecurity will have a steadily growing impact on business," says **Sakari Koikkalainen,** IT Security Manager with Valmet's IT infra services.

Cybersecurity will have to be extended beyond operational activities, as new challenges emerge. A sufficient level of cybersecurity will have been reached when cybersecurity threats are included in management and decision making. A cybersecurity strategy and management model, and technical and administrative controls should be created in support of business operations and form part of risk management. In addition to security

Risk-based cybersecurity management produces the most cost-effective result.

SAKARI KOIKKALAINEN
IT Security Manager, Valmet

controls, users' awareness of cybersecurity and security threats is a key factor in the creation of a good security culture.

"Cyber protection always requires some financial investment. That is why risk-based cybersecurity management produces the most cost-effective results," explains Koikkalainen.

Koikkalainen, who has long experience in telecommunications and data security management, began his career in the telecom sector in 1997. He joined Valmet's ICT management via Metso in 2006. His current tasks are aimed at developing Valmet's IT security.

Timely updates and patches

It is important at all times to understand what is being protected and from what. Any solutions introduced must not constitute cyber threats in themselves: they must be implemented securely and kept up to date.

"A focus on identities and data security are required in cybersecurity. Vulnerability management is an important part of preventive controls, in both technical and administrative terms," says Koikkalainen.

Once risk estimates and strategies have been drawn up, we need to ensure that the cybersecurity policy is implemented at the chosen level in all areas – no stable doors can be left open through which the 'cybersecurity horse' can bolt. It is only a matter of time before you pay the price if you leave any doors open. For example, any updates and patches published by software and application developers should be installed without unnecessary delays.

The continuous emergence of cloud services is bringing its special element to cybersecurity management. Their use must be consistent with the same data security strategy and policies as systems and applications within a company. So sufficient time and expertise should be devoted to planning and risk assessment before deploying cloud services. When considering the use of cloud services, thought should be given to business continuity and risk management, not just cost savings or agile features.

4
tips on how to succeed in cybersecurity

1. Pay attention to the cyber risk in business and decision-making.
2. Increase user awareness of cybersecurity.
3. Manage vulnerabilities both technically and administratively.
4. Make IT outsourcing systematically and business-oriented.

Better administration and detection

Since resource limitations form an everyday element of IT administration; sensible resource allocation is a key part of cost-effective cybersecurity.

For this reason, Koikkalainen views the outsourcing of IT administration to professionals as worthwhile when done in a business-oriented manner and planned with sufficient precision. This allows a company to target its own, often limited IT resources at the design of solutions for business activities and at ensuring that high added value is obtained from a high-quality service.

"I think that SOC services are one of the key cyberservices nowadays. These help to ensure a real-time overview of the cybersecurity situation. They also provide valuable information on the effective development and management of cybersecurity," says Koikkalainen.

Finnish companies have made significant progress regarding outsourcing. They have learned to buy services in the outsourcing of IT administration and other services are now commonplace.

"The major cybersecurity service innovations of the future will involve the detection of anomalies through cybersecurity services based on Big Data and artificial intelligence," says Koikkalainen. ✱

SAVING *energy and lives*

An interruption of the water, electricity or heating supply would directly affect almost all areas of life.

TEXT VESA KAARTINEN AND ESA LUOTO PHOTOS SHUTTERSTOCK AND KRISTIINA KONTONIEMI

A successful attack on the energy supply would quickly bring society to a halt. It would make life very cold, dark, dirty and difficult. Literally!

So it is no wonder that cyber and information security risks have become key talking points in the energy sector.

"It is becoming increasingly important to detect information security threats at the earliest possible stage. This would enable a rapid response and minimise damage," explains **Marko Metiäinen**, IT Service Manager at Jyväskylä Energy.

Companies face several cyber attacks per month on average. Most such attacks remained undetected or are only heard of when they make the headlines. In general, cyber attacks are only noticed months or even years after they begin.

According to Marko Metiäinen, the basic challenges are the same for energy companies as in any other sector, but the scope of responsibility is much broader and more inclusive.

> ***The key issue is to ensure the uninterrupted continuity of local energy production.***
>
> **MARKO METIÄINEN**
> IT Service Manager, Jyväskylä Energy

"The key issue is to ensure the uninterrupted continuity of local energy production and our own business operations. At any rate, this is ultimately about ensuring the daily security of every customer and organisation that we cover. Our tasks require constant emergency preparedness," Metiäinen summarises.

Digitalisation is an expertise renaissance

As digitalisation and the IoT progress, the discussion has moved from physical devices to overall infrastructure, and the related production, distribution and automation systems. Cyber risks are being increased by the easy blurring of risk responsibility in fragmented supply chains.

"Traditional antivirus software and network firewalls are no longer enough to keep information systems, networks and the data in them under companies' own control. As the number and range of security threats and risks

In contrast to the previous one-off audits, this enables us to anticipate the information and cyber security situation more comprehensively than before.

grow, new tools and experts who understand the big picture are continuously needed to combat them," comments Metiäinen.

Jyväskylä Energy's solution is to outsource information security monitoring and management services to the experts of CGI's Security Operations Center. The agreement will provide Jyväskylä Energy with access to CGI's global threat information and service network.

When CGI's SOC experts spot abnormal activity in Jyväskylä Energy's networks or systems, they analyse the findings that triggered the alarm and, based on the criticality of such findings, propose further measures.

"This service generates a real time snapshot of our network and information systems. In contrast to the previous one-off audits, this enables us to anticipate the information and cyber security situation more comprehensively than before. It also helps us to improve our preparedness for any incidents," Metiäinen explains.

According to the Government's Cyber Security Report, not all vital activities and maintenance-critical companies in society have adequate protection against cyber threats. There are also deficiencies in crisis tolerance.

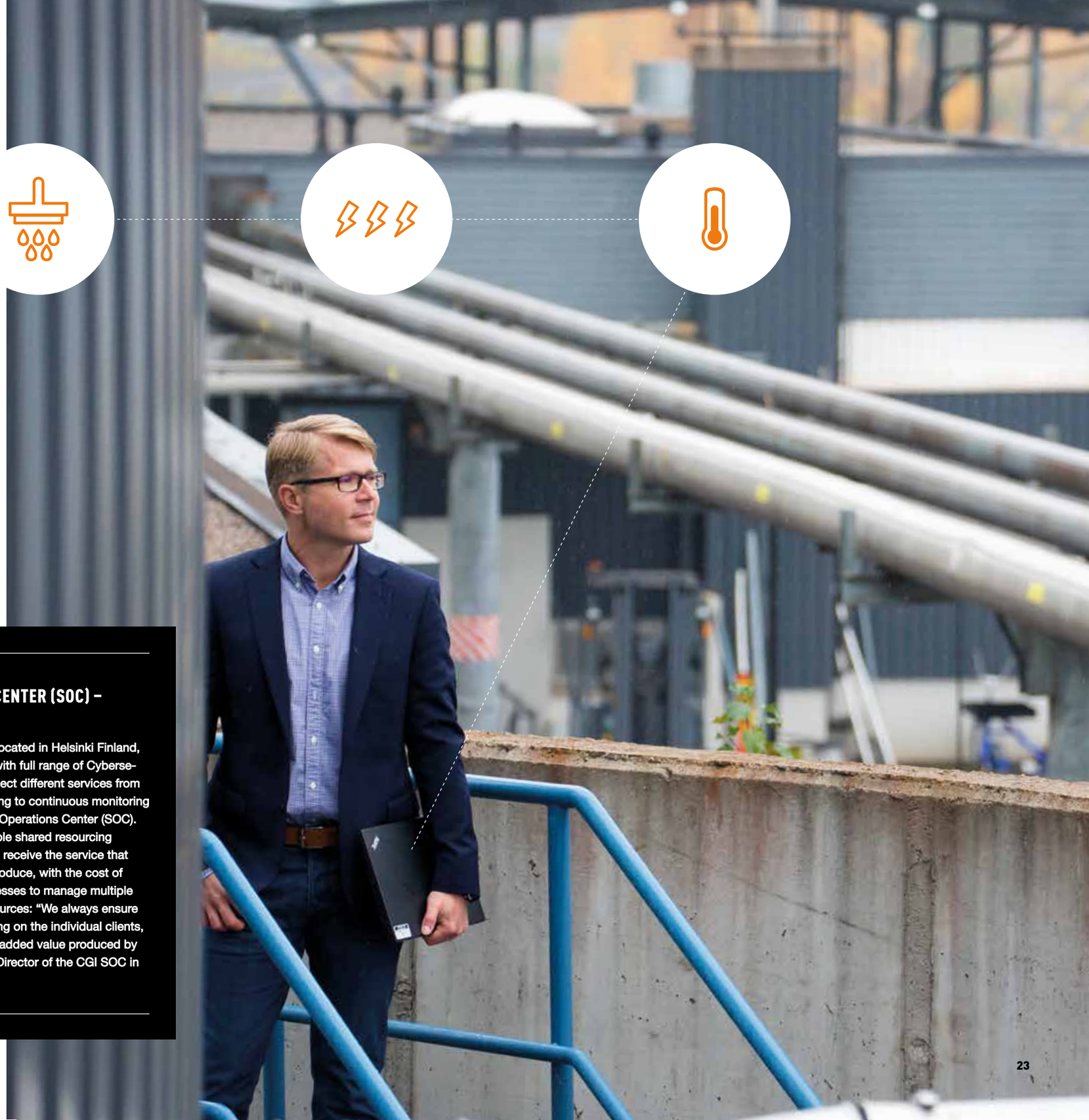
Metiäinen compares support for the SOC service to insurance cover. "Our priority is security of supply and operations in the Jyväskylä region. We cannot risk relying on technology alone." ✱

WOULD YOU LIKE TO ASK SOMETHING?
Mika Heino
+358 40 777 0370
mika.heino@cgi.com

CGI SECURITY OPERATIONS CENTER (SOC) – SHARED CYBER SERVICES

CGI'S SECURITY OPERATIONS CENTER, located in Helsinki Finland, provides Northern European clients with full range of Cybersecurity services. Organisations can select different services from Risk Management and threat modelling to continuous monitoring services often described as Security Operations Center (SOC).

SOC services are based on scalable shared resourcing and processes. This enables client to receive the service that would require ten different roles to produce, with the cost of one resource. With the efficient processes to manage multiple clients, CGI still relies on named resources: "We always ensure that we have a named analyst focusing on the individual clients, to ensure contextual knowledge and added value produced by the service", promised **Mika Heino,** Director of the CGI SOC in Helsinki.



LICENCE TO HACK

LähiTapiola uses white-hat hackers to seek out information security vulnerabilities. **Leo Niemelä,** Director, ICT Risk Management and Security, says that hacker collaboration is beneficial to all parties.

TEXT ARI RYTSY PHOTOS SHUTTERSTOCK AND SAMPO KORHONEN

The LähiTapiola open award for finding data security vulnerabilities, the Bug Bounty program, sprang from the desire to identify vulnerabilities more efficiently and proactively than before. Traditional methods were considered insufficient, despite the fact that LähiTapiola ensures the security of its eServices in a number of ways. Niemelä points out that even the most careful testing does not reveal every information security vulnerability. The more demanding the code is, the more likely is that some errors will only be found during the production stage.

"All coders are making the occasional error in the current digital upheaval. The Bug Bounty program provides more pairs of eyes when searching for such errors. This is not about blaming coders, but developing the data security of our services," says Niemelä.

LähiTapiola, the first Nordic financial company to begin the Bug Bounty program, did not rush headlong into collaboration with hackers. During the half-year design phase, the company conducted thorough risk analysis and threat modelling, since particular attention should be paid to the confidentiality and data protection of personal data in a strictly regulated business area.

The threats have not been realised – on the contrary. Experiences of the Bug Bounty program have been so good that it has been extended and the individual prize money has been raised from EUR 20,000 to 50,000. In practice, the prize is bigger the more significant the vulnerability's business impact would be. Under the new EU data protection regulation, a separate GDPR bonus is paid for detected vulnerabilities.

"EUR 18,000 is the biggest prize we've paid to date. Notification of the vulnerability and its correction was sent to the cyber security centre of the Finnish Communications Regulatory Authority, FICORA. From there, the information was shared with other companies," says Niemelä.

Producing the highest quality code is the everyone's goal.

LEO NIEMELÄ
Director, ICT Risk Management and Security, LähiTapiola

WOULD YOU LIKE TO ASK SOMETHING?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com

> ***Hackers make money and positive recognition of their skills through the Bug Bounty program. This is more attractive than doing something illegal and having to constantly look over your shoulder in fear of the authorities.***

Bug Bounty complements traditional information security

Bug Bounty vulnerability programs are one way of improving the security of corporate online services, which are sure to be targeted by unwanted hacking. The fear that a white hat with permission to hack services would change sides – and sell information on vulnerabilities on the black market – has not been realized.

"Hackers make money and positive recognition of their skills through the Bug Bounty program. This is more attractive than doing something illegal and having to constantly look over your shoulder in fear of the authorities," explains Niemelä.

Based on the positive experiences of the Bug Bounty program, LähiTapiola has brought more hackers on board through e.g its own Hack Day, where the security of the selected target system is probed by teams.

Bug Bounty complements, rather than replacing, traditional information security services. However, its use in LähiTapiola has led to savings in areas such as information security investments. It also plugs information security gaps in operations with various partners.

"LähiTapiola is continually developing new services and applications alongside its partners. Our customers' information security and the confidentiality of information are critical for us in everything we do," emphasises Niemelä.

The publicity attracted by the LähiTapiola Bug Bounty program is due to the company's decision to act as openly as possible. Similar projects are being quietly executed in Finnish companies, so that only they know the hackers who are testing their services. Regardless of the way in which the Bug Bounty program is implemented, Niemelä is convinced of its benefits. In addition to improved service security, such benefits can be seen in the development of the company's security culture and better internal security.

"Producing the highest quality code is everyone's goal. Any vulnerabilities identified are used to help develop the skills of programmers and security testers," he says.

4x

Take the advantage of hackers

1. Start with planning, conduct risk analysis and threat modelling.
2. Pay attention particularly to confidentiality and data privacy.
3. Take advantages of the prizing and utilization of hackers.
4. Use findings to train and develop programmers.

ICT partners are included in the program

That is why a specially designated team, including representatives of the company's ICT partners alongside its own security experts, is in charge of running the Bug Bounty program in LähiTapiola. The involvement of partners has brought a broader understanding of data security and enabled a rapid response to identified recoding needs.

The program has developed its own impetus after the tentative early stage. LähiTapiola's current ICT contracts refer to the fact that the external interfaces of its services are covered by the Bug Bounty program.

No additional recruitment needs have arisen due to integrating the successful vulnerability program with daily operations: ease of use, speed and cost-effectiveness can be added through external partners who are familiar with the applications used in a company.

"The use of programs such as Bug Bounty are sure to increase, particularly for customer interface solutions. In this area, hackers are one more tool in the battle for information security," sums up Niemelä. *

Leo Niemelä, Director, ICT Risk Management and Security, says that hacker collaboration is beneficial to all parties.

Cybersecurity seminar & SOC Tour

23rd of January 2019 at 12:00–18:00
CGI office, Helsinki, Finland

Welcome to CGI's Cybersecurity Seminar and hear our clients', partners' and experts' views on current trends and information on what kind of security measures are needed to tackle cybersecurity challenges today. As part of the seminar, you will have an opportunity to visit one of our eight Security Operations Centers (SOC) globally.

The seminar is targeted for IT, business and security leaders.

Read more and register: cgi.fi/cyberseminar

You are also welcome to join our annual **Ratkaisu19 seminar** the next day, 24th of January, at Finlandia Hall, Helsinki. Ratkaisu is one of the biggest IT and business seminars in the Nordics. In Ratkaisu19, you will hear speeches on how organisations invest in digitalization and growth, and what kinds of strategies businesses have for developing their competitiveness in the digital age.

Read more and register: ratkaisu.cgi.fi/en

CGI