C*

*CYBERSECURITY 18
Ratkaisu Magazine Issue Excerpt

CGI
Experience the commitment®

Take care of THE BASICS

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

BY ARI RYTSY PHOTOS BY 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 infrastructure services.

Cybersecurity will have to be extended beyond operational activities, as new challenges emerge. A sufficient level of cybersecurity maturity will have been reached when cyber threats are included in management plans and decision making. A cybersecurity strategy and management model, and technical and administrative controls should be created in support

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 extensive 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 threats. 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 is 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 will only be a matter of time before you pay the price for leaving any doors open. For example, any updates and patches published by software and application developers should be installed without unnecessary delays.

4
tips on how to succeed in cybersecurity

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

The continuous emergence of cloud services is bringing a special element to cybersecurity management. Use of these services must be consistent with the same data security strategy and policies that are applied to systems and applications within the company. 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.

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 experts as worthwhile when done in a business-oriented manner and planned with sufficient precision. This allows a company to focus its own, often limited IT resources on designing solutions for business activities and ensuring that high added value is obtained from a high-quality service.

"I think that SOC services are one of the key cyber services nowadays. They 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 with using outsourcing services including the outsourcing of IT administration and other services, which 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. ✱