SECURITY AND FIRE INDUSTRY

CYBERSECURITY

THREAT OR OPPORTUNITY ?
IT'S UP TO YOU !

AN INFORMATION BROCHURE FOR PROFESSIONALS IN THE SECURITY AND FIRE INDUSTRY

CoESS

euralarm

CYBERSECURITY – TOP PRIORITY

Cybersecurity is a top priority for businesses and governments. The increasingly sophisticated cyberattacks involving malware, phishing, machine learning and artificial intelligence, cryptocurrency and more are placing corporations', governments' and individuals' data and assets at risk. Many large, but also small enterprises already have structures and people in place to enhance resilience against such risks. Still, many others have the wrong impression that enhanced cybersecurity demands a lot of resources. Another myth is that cybersecurity and physical security are two different worlds. The "frontier" between the physical and the cyber world is an illusion and furthermore neither can be effective without the other. For example access control to important IT equipment is highly important.

Today, any device connected to a network or people working with this equipment have the potential to take down an entire network or business. This can be your own business, but may also be your customers' business. That's because more and more businesses have connected devices. This includes not only computers, mobile phones and tablets; but additionally any connected peripheral devices such as cameras, WiFi printers or the use of a USB memory stick. All these can create cybersecurity risks.

Taking measures to enhance resilience against cyberthreats is crucial - for business continuity, security of data and assets, as well as the reputation of both your business and your customers'. Today, if you purchase the correct products you have the right tools at hand to provide you with a level of protection such as passwords, encryption and secure databases. Together with stringent internal cybersecurity rules and procedures, your business' cyber-resilience can be enhanced tremendously. Still, many do not realise the importance of these, sometimes simple, measures.

Whether you are a manufacturer, an installer, a service provider or a security guard – you have to ensure that you understand the importance of human factors in achieving an acceptable level of cybersecurity and leverage your available resources. You need to protect both your own and your customers' data and equipment.

The aim of this paper is to create awareness that, with the right security measures, cyberthreats can be mitigated. It looks at the whole chain, from security equipment, design and installation to security services. It gives recommendations on the role of employees and end-users in carrying out security measures to minimise cybersecurity risks. This requires an awareness that each part of the security chain needs to implement its own measures. The paper also highlights what is already being done to mitigate existing risks and what you can do in order to ensure the integrity of the chain.

Businesses that make cybersecurity a priority protect themselves and their customers; they are sending the right message to their employees, their customers, and more generally protect their brand, reputation and income. It is up to you to take cybersecurity seriously.

DID YOU KNOW THAT:

68% of global companies say cyber-security risks are increasing, while only 30% are confident in the security of their network [1]

Cybercrime could cost companies globally **$5.2** trillion of future revenues over the next five years [1]

80% of EU businesses have experienced at least one cybersecurity incident [2]

1 Abbosh O., Bissell K. (2019) : "Securing the Digital Economy".
2 Europol (2017): Internet Organised Crime Threat Assessment.

WHAT EXACTLY IS CYBERSECURITY?

"Cybersecurity is the protection of connected systems, including hardware, software and data, against cyberattacks from remote (internet based), local (bluetooth and wireless), or internal (malicious or negligent staff) threats. In a computing context, security comprises cybersecurity and physical security - both are used by enterprises to protect against unauthorised access to data and other computerised systems." [3]

This includes much more than we think, including the risk for your own business. You may think that what you are doing is unaffected by cyberthreats, however this may simply not be true. Fire alarm systems, access control systems, intrusion alarm systems and CCTV systems are either already or quickly becoming an integral part of an IT network.

Cybersecurity is everyone's responsibility in the supply chain. It is therefore important that everybody understands their role in the chain because your complete system is as strong as its weakest part.

As graphically represented in the image above, cybersecurity is a cyclic process which never ends.[4]

To keep your business and your customers' business cybersecure you need to play the game by the rules. Password changes, software updates, education and awareness are key to maintain an effective cybersecurity strategy.

3 https://searchsecurity.techtarget.com/definition/cybersecurity
4 Source graphic: https://www.nist.gov/blogs/manufacturing-innovation-blog/dealing-cyber-attacks-steps-you-need-know

WHERE TO FIND MORE INFORMATION

Austria	Federal Ministry for Digitalisation www.onlinesicherheit.gv.at
Belgium	Centre for Cybersecurity Belgium www.ccb.belgium.be
Bulgaria	National Center for Incident Response in Information Security www.govcert.bg
Croatia	Information Systems Security Bureau www.zsis.hr
Cyprus	National Computer Security Incident Response Team www.csirt.cy
Czech Republic	National Cybersecurity Center www.govcert.cz
Denmark	Center for Cybersecurity www.feddis.dk/cfcs
Estonia	Information System Authority www.ria.ee
Finland	National Cybersecurity Centre www.kyberturvallisuuskeskus.fi
France	National Agency for the Security of IT Systems www.ssi.gouv.fr
Germany	Federal Agency for IT Security www.bsi.bund.de
Hungary	National Cyber Defence Institute www.nki.gov.hu
Ireland	National Cybersecurity Centre www.ncsc.gov.ie
Italy	CERT Nazionale www.certnazionale.it
Latvia	Information Technology Security Incident Response Institute www.cert.lv
Lithuania	National Cybersecurity Centre www.nksc.lt
Luxembourg	Computer Incident Response Centre www.circl.lu
Malta	Critical Infrastructure Protection Directorate www.maltacip.gov.mt
Poland	CERT Polska www.cert.pl
Portugal	National Cybersecurity Centre www.cncs.gov.pt
Romania	CERT Romania www.cert ro.eu
Slovakia	Computer Emergency Response Team www.sk cert.sk
Spain	National Cybersecurity Institute www.incibe.es
Sweden	Computer Security Incident Response Team www.cert.se
Switzerland	Reporting and Analysis Centre MELANI www.melandi.admin.ch
The Netherlands	National Cybersecurity Centre www.ncsc.nl
United Kingdom	National Cybersecurity Centre www.ncsc.gov.uk

THE HUMAN FACTOR: KEY FOR A RESILIENT CYBERSECURITY FRAMEWORK

FOR YOUR BUSINESS

- Ensure that you know your key business systems and that you understand what the impact would be if these systems became compromised
- Set up an internal cybersecurity framework, and clearly assign information security tasks to one or more dedicated staff members
- Create and maintain a cybersecurity culture within the entire company:
  - Screen, monitor and audit all personnel in an appropriate way
  - Provide regular mandatory cybersecurity hygiene training among all staff members including product training if necessary
  - Set in place rules and procedures which, if implemented as instructed, will mitigate cybersecurity risks - for example for:
    - Cybersecurity responsibilities and accountabilities
    - Accessing internet/public websites (e.g. white lists of websites)
    - Data privacy and permissions for accessing data
    - Email, password and USB memory stick policies
    - Software updates and anti malware measures
- Build co-operative frameworks between stakeholders along the security chain
- Set in place response and business continuity plans:
  - Designate a Business Continuity Team, incl. responsibilities, rules and procedures for response actions
  - Prepare and test business continuity plans to deal with different events
  - Ensure effective data back-up policy
  - Ensure all relevant stakeholders are involved in contingency planning
- Ensure that measures are taken to manage risks, regularly evaluate rules and procedures, and adopt corrective measures where appropriate, incl. risk assessments and stress tests on consequences of a breach

FOR YOUR CUSTOMERS

- Make your customers aware of cybersecurity risks
- Agree on activities and controls, including mutual responsibilities, to manage the risks
- Ensure that these responsibilities are sustained throughout the lifetime of the solution, e.g. by a service agreement
- Assign information security tasks to one or more dedicated staff members
- Update contact records on a frequent basis
- Regularly review cybersecurity strategies and requirements
- Train customer personnel
- Set in place joint back-up procedures

CYBERSECURITY RISKS AND SOLUTIONS - STEP-BY-STEP

PRODUCT

PROJECT DESIGN

INSTALLATION

RISKS

A majority of the product and software manufacturers have taken a holistic approach to cybersecurity. Start with establishing a secure architecture and design to ensure a solid product foundation. Secure architecture is the discipline that specifies and assures compliance with security measures, requirements and implementation guidelines. It includes secure development, cyber-protection, testing procedures, configuration guidelines, user / installer education and finally rapid response to security issues.

Cybersecurity in a safety and/or security project design is to be considered in the context of overall risk management, including information security and business continuity, and IT strategy. The project design should include a cybersecurity framework, and this should be adapted and fit for purpose. It is therefore essential to understand the customer's security objectives and requirements. Structured project and system design processes begin with a security risk assessment to find and assess the impact of security related threats and vulnerabilities.

Installation refers to both the project installation and commissioning phases. During the installation phase, all cybersecurity hardening guidelines defined in the Project Design including the ones provided by the product manufacturers are to be implemented. This includes changing default passwords, system access credentials and user accounts to fit to the customer's operations. Furthermore, all devices connected to the security network need to be configured to reduce potential vulnerabilities. Configuration options include defining applications to install, activating or deactivating settings, and setting up user and system accounts as well as setting access rights, and the use of encryption.

SOLUTIONS

HARDWARE CHOICE

- Security by design
- Certified and compliant with the latest standards

FIRMWARE / SOFTWARE

- Secure and up-to-date operating system
- Security software updates and upgrades
- Password protection and encryption
- System lock

DESIGN

- Use of cyber-resilient products and services
- Fit for purpose cybersecurity framework
- Compliant with the latest standards
- Network firewall setting
- Encryption on network / database
- Physical security for vulnerable network devices and cabling
- Operational requirements
- Resilience (e.g. battery back-up)
- Cyber-competence of the end user

HARDWARE CHOICE

- Security by design
- Tamper protection
- Secure network

FIRMWARE / SOFTWARE

- Configuration options
- Password protected
- Network knowledge
- Commissioning / testing
- End user training
- Operating instructions
- Emergency telephone numbers

OPERATIONAL CONTINUITY

Operational continuity is guaranteed by first-in-line technical support and/or from alarm response support services in an Alarm Receiving Centre (ARC). The former receives system deficiency input and decides on a technical response; the latter receives and identifies an incoming alarm and decides on an alarm service response. To avoid that hackers get access to alarm systems, hard and software for entry point technologies and alarms need to be constantly protected and checked, and security and alarm transmission system events need to be logged. System integrity should be constantly checked and monitored.

HARDWARE CHOICE

- Security by design
- Secure and protected operating system, including all entry point and alarm systems
- Certified and compliant with the latest standards
- Decommissioning of technical obsolence
- Ongoing maintenance

FIRMWARE / SOFTWARE

- Upgradable
- Password protected
- Hardened IT infrastructure / firewalls
- Security and alarm transmission system event logs
- Cybersecurity checks before and after updates

RESPONSE

Response is the follow-up on an alarm / incident. It can be initiated in different ways. An ARC may first evaluate the alarm / incident remotely, which also relies on data that can get hacked or leaked in the process. The ARC may then have to notify the customer and law enforcement to report the alarm, potentially with the support of an on-site guard. Insufficient cybersecurity on all levels can result in unnoticed manipulated and leaked communication, compromised data privacy and access control of the asset, and delayed response, certainly if all devices along the security chain are not regularly updated and checked to have highly resilient soft- and hardware.

HARDWARE CHOICE

- Security by design
- Protected and secure operating, communication and access control systems
- Certified and compliant with the latest standards
- Regular checks

FIRMWARE / SOFTWARE

- Upgradable
- Password protected
- Hardened IT infrastructure / firewalls
- Resilient and secure operating, communication and access control systems (GPS-steered, time-limited codes) across the entire security chain
- Cybersecurity checks before and after updates

IGNORANCE OF CYBERSECURITY RISKS

INADEQUATE PASSWORD MANAGEMENT

INSUFFICIENT MAIL AND WEB SECURITY

MALWARE

POOR VULNERABILITY MANAGEMENT

TOP 5 CYBERSECURITY EXPOSURES

IGNORANCE OF CYBERSECURITY RISKS

Over the past years we have seen an increasing number of high-profile cyberattacks in all kinds of industries. Still, many are not aware of the size and severity of the threat that cybercriminals can pose to their own business. It is up to all of us to change that.

INADEQUATE PASSWORD MANAGEMENT

Passwords continue to be a major security risk for organisations. This is often due to easily hacked codes and stolen or lost passwords that can leave the door to your IT system wide open.

INSUFFICIENT MAIL AND WEB SECURITY

Everyone of us has already seen them: phishing emails. Their goal is to entice the reader to click on a link or to open an attachment - for example by notifying you of bank transfers, lottery wins or package shipments. Phishing emails are still a very common tactic of hackers to steal data or infect systems with malware.

MALWARE

Your system can get infected with malware in various ways, for example through phishing emails, insecure websites or contaminated USB memory sticks. Often, this malicious software is installed on your computer without you noticing it. The software can stay dormant over months before stealing data, including passwords, or even taking over entire systems.

POOR VULNERABILITY MANAGEMENT

Hackers are always looking for new vulnerabilities in systems to exploit. Nowadays, software is written and released quicker than ever before. As a consequence, cybersecurity vulnerabilities emerge if the vendor doesn't provide an update that addresses these weaknesses or if businesses don't update their software regularly.

ABOUT EURALARM

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres.

Founded in 1970, Euralarm represents over 5 000 companies, employing 700 000 people, within the fire safety and security industry with an estimated revenue of € 67 billion. Euralarm members are national associations and individual companies from across Europe.

ABOUT CoESS

CoESS acts as the voice of the Security Industry. The main objective of CoESS is to represent and support the growth of an industry that delivers solutions of high quality and professionalism, focused on the selection and development of qualified staff and technology. The core values of CoESS are Quality, Safety, Compliance and Trust. It is the umbrella organization for 23 national private security employers' associations, of which 18 in EU Member States. CoESS is recognised by the European Commission as a European sectoral social partner and is active in a constructive Social Dialogue with UNI Europa.