Cyber security

The ABC of cyber security

The aim of any cyber security strategy is to protect as many assets as possible and especially the most important – the "crown jewels". Since it is not feasible, sensible or even efficient to try to protect everything in equal measure, it is important to identify what is valuable and needs greatest protection, identify vulnerabilities, then to prioritize and to erect defence-in-depth architecture that ensures business continuity. Defence-in-depth involves the coordination of multiple security countermeasures, based on the military principle that a multi-layered defence system is more difficult to penetrate.

Installing secure technology is of crucial importance but alone it will not ensure resilience. It is mostly about understanding and mitigating risks in order to apply the right protection at the appropriate points in the system. It is vital that this process is very closely aligned with organizational goals because mitigation decisions may have a serious impact on operations. Ideally, it would be based on a systems approach that involves stakeholders from throughout the organization.

There are four steps to take in order to deal with the risk and consequences of a cyber-attack:

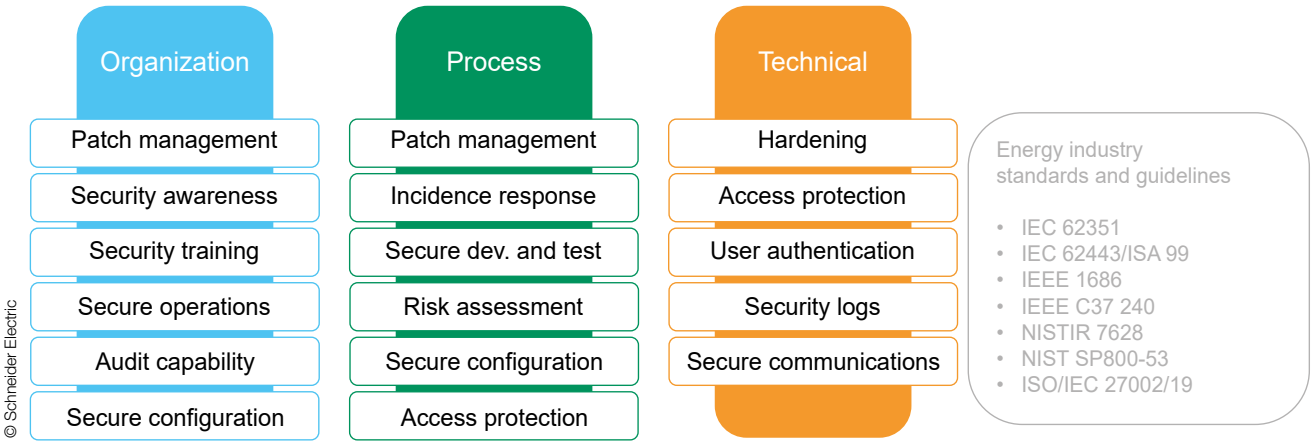
- Understand the system, what is valuable and what needs most protection
- Understand the known threats through threat modelling and risk assessment
- Address the risks and implement protection with the help of International Standards, which reflect global best practices
- Apply the appropriate level of conformity assessment – assessment, testing and certification – against the requirements

Another way of thinking of this is as the "ABC" of cyber security:

- "A" for assessment
- "B" for best practices to address the risk
- "C" for conformity assessment for monitoring and maintenance

A risk-based systems approach increases the confidence of all stakeholders by demonstrating not only the use of security measures based on best practices, but also that an organization has implemented the measures efficiently and effectively. This means combining the right standards with right level of conformity assessment, rather than treating them as distinct areas. The aim of the conformity assessment is to assess the components of the system, the competencies of the people designing, operating and maintaining it, and the processes and procedures used to run it. This may mean using different kinds of conformity assessment – ranging from corporate self-assessment to relying on the declarations of suppliers to independent, third-party assessment and testing – whichever are most appropriate according to the different levels of risk.

Three axes of cyber security



The IEC advocates a holistic approach to building cyber resilience, combining best practices with testing and certification. A holistic approach incorporates people, processes and technology: the three axes of cyber security. Cyber security protection technologies only really work when combined with proper organization, processes and procedures. This requires an ongoing effort and recurring investment, not least in the training of people.

It is essential to start considering security threats during the initial design and development phase. In many instances, organizations only look at security after implementation, rather than building cyber resilience from the beginning of the development lifecycle.

In response to the growing threat, many organizations have based their cyber security strategies on compliance with mandatory rules and regulations. International Standards are increasingly adopted by countries at the regional and national level, either in full, without any variation, or in part, with supplementary requirements contained in national standards. This may lead to improved security, but cannot address the needs of individual organizations in a comprehensive manner, which can only be achieved through a process of risk assessment that addresses not only external challenges, but also internal weaknesses.

This requires conformity assessment. Standards and conformity assessment are like two sides of a coin. Only together do they have value.

Critical vs. non-critical systems

Official reports, formal studies and countless stories from trusted news media around the world testify to the fact that cyber attacks are increasing, both in level and sophistication. Many of the attacks are against systems, facilities, technologies, networks, assets and services essential to health, safety, security or economic well-being.

It is important to differentiate between critical and non-critical systems and infrastructure. Cyber attacks against home networks and consumer devices are serious for those directly concerned, but not vital to a larger population. If malicious actions target home thermostats or automated blinds, for example, this can be annoying for users. In the worst case scenario, these attacks may open hidden gateways (e.g. door locks), but they do not bring down critical infrastructure – entire systems that would affect a country's ability to function normally, such as electricity generation, water distribution or healthcare.

In a world where cyber threats are becoming increasingly common, being able to apply a specific set of International Standards combined with a dedicated and worldwide certification programme, is a proven and highly effective approach to ensuring long-term cyber resilience. A concerted effort in international standardization and conformity assessment offers many advantages. Applying standards alone will not result in an "achieved cyber-secure state".

IT and OT: complementary but different

Attacks targeting critical infrastructure have provoked power outages and compromised sensitive data, as well as evoking nightmare scenarios involving environments such as water supply systems, petrochemical installations, nuclear power plants and transport infrastructure systems, which are all dependent on operational technology (OT) and to varying degrees, information technology (IT). The primary focus of IT is data and its ability to flow freely and securely. It is fluid and has many moving parts and gateways, making it more vulnerable and offering a large surface for a greater variety of constantly evolving attacks. Defending against attacks is about safeguarding every layer, continuously identifying and correcting weaknesses to keep data flowing.

On or off

In manufacturing and critical infrastructure such as electricity generation, water management, transportation, or healthcare, operational technologies ensure the correct execution of all actions. Everything in OT is geared to physically moving and controlling devices and processes to keep systems working as intended, with a primary focus on security and increased efficiency. For example, OT helps ensure that a generator comes online when there is an increase in electricity demand, or an overflow valve opens when a chemical tank is full, to avoid a spill of hazardous substances. When OT systems are under attack, the physical effects of incidents are generally magnitudes greater than those caused by attacks on IT systems. Protecting the automated system of an oil refinery has a different impact from that of the customer database of a bank. Any interruption or malfunction of an OT system can result in injuries, faulty goods, spills or when an electricity grid goes offline, in the shutdown of all essential services.

In the past IT and OT had separate roles. OT teams were used to working with closed systems that relied heavily on physical security mechanisms to ensure integrity. With the emergence of the industrial Internet of Things (IIoT) and the integration of physical machines with networked sensors and software, the lines between the two are blurring. As more and more objects are connected, communicate and interact with each other in the Internet of Things (IoT), there has been a surge in the number of endpoints and potential ways for cyber criminals to gain access to networks and infrastructure systems. Simply put, the convergence – the combination of two or more different technologies in a single device or system – of the once separate domains has made cyber security more technically complex.

Protecting supply chains

It is thought that the vast majority of cyber breaches may originate in supply chains. Generally speaking, a supply chain is the journey that products and services make from supplier to customer. A supply chain is a system that encompasses organizations, people, activities, information and resources.

As defined in ISO/IEC 27036-1, "the IT supply chain consists of a set of organizations with linked sets of resources and processes, each of which acts as an acquirer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement." A definition of supply chain for critical infrastructure, such as power grids, transportation systems and smart manufacturing, is more complex as it comprises not only IT, but also the OT supply chain. This includes people (developers, suppliers, vendors and staff working on OT) and processes, as well as products – components and systems central to OT, such as industrial automation and control systems (IACS) and increasingly, IoT elements.

Industrial and critical infrastructure assets are most at risk, but protecting supply chains is of crucial importance for all businesses and enterprises. The IEC has developed standards and conformity assessment schemes to protect supply chains.

Generic and flexible: horizontal standards

The most effective defences rely on both horizontal and vertical standards. Horizontal standards are generic and flexible, while vertical standards cater to very specific needs.

The ISO/IEC 27000 family of standards helps to protect purely IT systems and ensures the free flow of data in the virtual world. It provides a powerful, horizontal framework for benchmarking against best practices in the implementation, maintenance and continual improvement of controls. In contrast, IEC 62443 – an indispensable series of standards that establishes precise cyber security guidelines and specifications applicable to a wide range of industries and critical infrastructure environments – is designed to keep OT systems running in the physical world.

The IECEE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) includes a programme that provides certification to standards within the IEC 62443 series.

IEC 62443 is well known to cyber security experts for adopting a layered, defence-in-depth approach. The series is also used in the transport sector while the International Maritime Organization (IMO) refers to IEC 62443 in a set of cyber security guidelines for ships. Shift2Rail, an initiative that brings together key European railway stakeholders, has selected IEC 62443 for the railway sector. This series is also compatible with the US National Institute of Standards and Technology (NIST) cyber security framework.

Custom solutions: vertical standards

Complementing the horizontal standards are custom solutions designed to protect specific domains and to keep industry and critical infrastructure assets safe. For example, there are vertical standards covering the specific security needs of the nuclear industry, industrial automation, healthcare and the maritime industry, among others. Here is a selection of them:

- IEC Subcommittee (SC) 45A together with the International Atomic Energy Agency (IAEA) is developing specific standards for nuclear power plants by using the IEC 62443 series and tailoring specific parts of ISO/IEC 27001 and ISO/IEC 27002 to fit the nuclear context
- IEC SC 45A has developed IEC 62645 to protect microprocessor-based information and control systems
- IEC Technical Committee (TC) 57 develops, among many others, the IEC 61850 series of publications for communication networks and systems for power utility automation, and the IEC 60870 series for telecontrol equipment and systems
- IEC TC 80 has developed the IEC 61162 series for maritime navigation and radiocommunication equipment and systems

A framework for building resilience

The IEC provides a framework incorporating multiple standards covering a variety of IT and OT technologies. More than 200 IEC cyber security standards enable organizations to increase their resilience and robustness in the face of a rapidly-evolving threat. The framework integrates horizontal standards that are suitable for all sectors, such as ISO/IEC 27000 or IEC 62443, with vertical standards written for specific sectors. Furthermore, the IEC is the only organization in the world that provides an international and standardized approach to testing and certification. For cyber security such services are supplied by the IECEE. The IECEE industrial cyber security programme tests and certifies cyber security in the industrial automation sector, in accordance with the IEC 62443 series.

Increasing numbers of organizations are turning to third-party certification to ensure that they have a solid information security management system (ISMS) in place which conforms to ISO/IEC 27001. ISO/IEC 27006 provides the requirements that certification and registration bodies need to meet in order to offer ISO/IEC 27001 certification services.

Both the IEC Standardization Management Board (SMB) and the Conformity Assessment Board (CAB) have identified cyber security as a strategic priority. The SMB works with an advisory committee, while the CAB relies on two working groups to coordinate activities related to testing and certification. In addition, an IECEE committee focuses on issues related to conformity assessment to the IEC 62443 series.


15,56 C
33,94 C
32,13 C
Date XX-XX-XXXX
Time XX:XX
Job WW25D76
Automation machine

About the IEC

Key figures

172
members and affiliates

>200
technical committees

20 000
experts from industry, test and research labs, government, academia and consumer groups

>10 000
international standards published

4
global conformity assessment systems

>1 million
conformity assessment certificates issued

>100
years of expertise

The IEC, headquartered in Geneva, Switzerland, is the world's leading publisher of international standards for electrical and electronic technologies. It is a global, independent, not-for-profit, membership organization (funded by membership fees and sales). The IEC includes 172 countries that represent 99% of world population and energy generation.

The IEC provides a worldwide, neutral and independent platform where 20 000 experts from the private and public sectors cooperate to develop state-of-the-art, globally relevant IEC International Standards. These form the basis for testing and certification, and support economic development, protecting people and the environment.

IEC work impacts around 20% of global trade (in value) and looks at aspects such as safety, interoperability, performance and other essential requirements for a vast range of technology areas, including energy, manufacturing, transportation, healthcare, homes, buildings or cities.

The IEC administers four conformity assessment systems and provides a standardized approach to the testing and certification of components, products, systems, as well as the competence of persons.

IEC work is essential for safety, quality and risk management. It helps make cities smarter, supports universal energy access and improves energy efficiency of devices and systems. It allows industry to consistently build better products, helps governments ensure long-term viability of infrastructure investments and reassures investors and insurers.

A global network of 172 countries that covers 99% of world population and electricity generation

Offers an affiliate country programme to encourage developing countries to get involved in the IEC free of charge

Develops international standards and runs four conformity assessment systems to verify that electronic and electrical products work safely and as they are intended to

IEC International Standards represent a global consensus of state-of-the-art know-how and expertise

A not-for-profit organization enabling global trade and universal electricity access

Further information

For further information, please visit the IEC website at www.iec.ch. In the “Who we are” section, you can contact your local IEC National Committee directly. Alternatively, please contact the IEC Central Office in Geneva, Switzerland or the nearest IEC Regional Centre.

Global

IEC – International Electrotechnical Commission
Central Office
3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

IEC Regional Offices

IEC-AFRC – Africa Regional Centre
7th Floor, Block One, Eden Square
Chiromo Road, Westlands
PO Box 856
00606 Nairobi
Kenya

T +254 20 367 3000 / +254 20 375 2244
M +254 73 389 7000 / +254 70 493 7806
Fax +254 20 374 0913
eod@iec.ch
fya@iec.ch

IEC-APRC – Asia-Pacific Regional Centre
2 Bukit Merah Central #15-02
Singapore 159835

T +65 6377 5173
dch@iec.ch

IEC-LARC – Latin America Regional Centre
Av. Paulista, 2300 – Pilotis Floor
Cerqueira César
São Paulo – SP – CEP 01310-300
Brazil

T +55 11 2847 4672
as@iec.ch

IEC-ReCNA – Regional Centre for North America
446 Main Street, 16th Floor
Worcester, MA 01608
USA

T +1 508 755 5663
Fax +1 508 755 5669
tro@iec.ch

IEC Conformity Assessment Systems

IECEE / IECRE
c/o IEC – International Electrotechnical Commission
3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
secretariat@iecee.org / secretariat@iecre.org
www.iecee.org / www.iecre.org

IECEx / IECQ
The Executive Centre
Australia Square, Level 33
264 George Street
Sydney NSW 2000
Australia

T +61 2 4628 4690
Fax +61 2 4627 5285
info@iecex.com / info@iecq.org
www.iecex.com / www.iecq.org

Cyber security:2018-09(en)