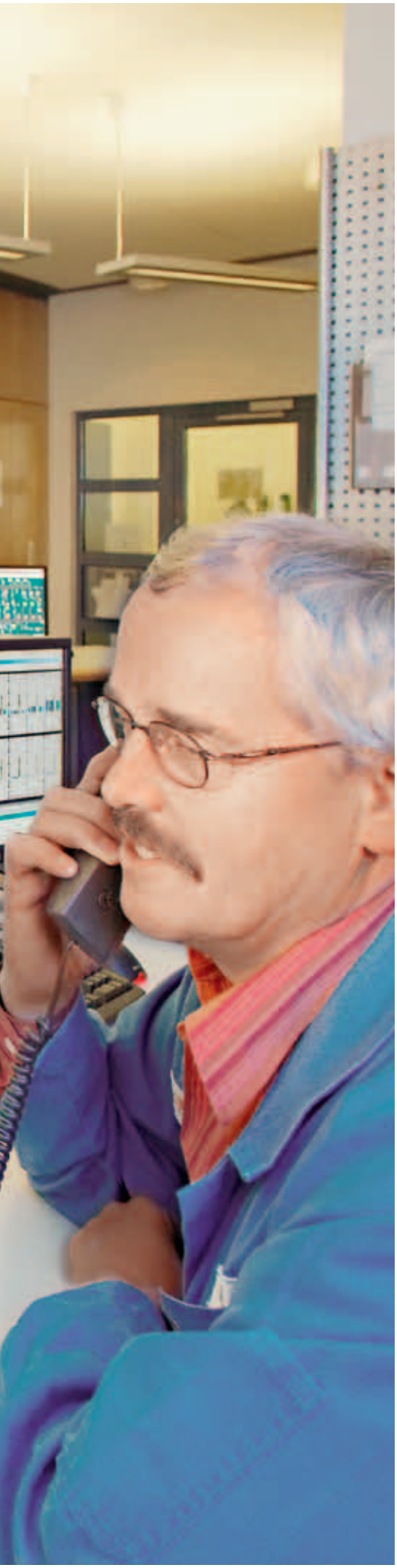


Protection from cyber threats

Can utilities and industries afford a cyber security breach?

PATRIK BOO – The intensity of cyber attacks on IT systems increases with every passing day. Worryingly, growing connectivity and hacker sophistication are making IT systems more vulnerable to such intrusions. Targets that have, until recently, remained relatively unscathed, or at least unnoticed, are the systems that oversee industry processes around the world. The highly sophisticated attack by the Stuxnet malware and other control system incidents have raised general awareness of control system vulnerability. If a control system is attacked, or even unintentionally compromised, the result could include regulatory violations, equipment damage, production loss, harm to the environment, or public and employee endangerment. In response to the potential threat and consequent customer demand, ABB has created Cyber Security Fingerprint, a noninvasive service that significantly helps to reduce a control system's risk of attack.

Title picture
Today's "wired" environment presents cyber security challenges for owners of control systems. ABB's Cyber Security Fingerprint provides a comprehensive solution.

As cyber crime costs are two to three times higher than the cost of safeguards, proactively investing in cyber security makes good sense.

Today's control systems are more vulnerable to cyber threats than ever due to increased interconnectivity, cloud computing and sharpened hacker skills. Whereas enterprise IT was always a favored hacking target, hackers' attention is now increasingly turning to control systems. Adding further urgency to the situation is the fact that emerging economies are creating a proliferation of control systems.

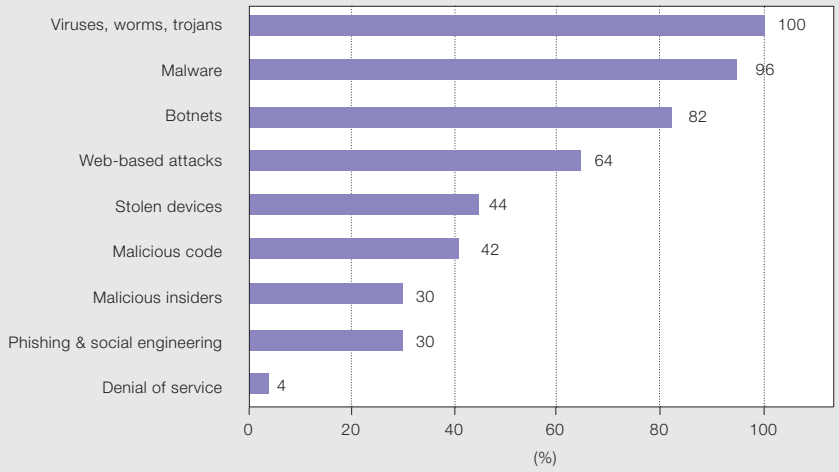
Attacks on control systems can cause havoc:

- In a sewage treatment plant in Australia, a disgruntled former contractor gained access to the plant's control system and flooded the surrounding area with millions of liters of untreated sewage, contaminating parks, rivers and the grounds of a hotel.
- In Australia, the "Sasser" worm infected the signaling and control system of RailCorp, halting all trains for the day and stranding 300,000 Sydney commuters.
- The control systems of water utilities in the US states Illinois and Texas were allegedly hacked. In Illinois, a water pump was repeatedly turned on and off until it burned out [1]. Shortly afterwards, a hacker posted screenshots of himself logged into the control system of a Texan water utility to demonstrate how easily the Illinois control system – or any other – can be hacked.
- The safety monitoring system of the Davis-Besse nuclear power plant in Ohio was infected with the "Slammer" worm in January 2003, disabling it for five hours. The worm bypassed the plant's firewalls via a contractor's laptop computer that was connected to the power plant's network. Fortunately, the nuclear plant was shut down for scheduled maintenance at the time. However, the worm raced through the Internet and caused a denial of service on some Internet hosts, dramatically slowing general Internet traffic. In addition to the nuclear plant, the worm infected almost 75,000 other victims within 10 minutes, including a power company control system via a virtual private network (VPN), a petroleum plant control system via a laptop, and a paper machine operator station via a dial-up modem. It is estimated to have caused more than $1 billion in damage.

A 2011 study by the Ponemon Institute on cyber crime in large US-based multinational organizations quantifies the financial impact of cyber attacks and highlights how they can seriously damage an organization's bottom line [2]. The study found that the median cost to a company of cyber attacks is $5.9 million per year, though this figure ranged from $1.5 million to $36 million. These costs are not expected to decline. The $5.9 million figure represents an increase of 56 percent from 2010.

According to the Ponemon report, a benchmark sample of 50 organizations experienced 72 discernible and successful cyber attacks per week in 2011, which translates to 1.4 successful attacks per benchmarked organization each week. This represents a 44 percent increase in successful attacks from the previous year. Virtually all organizations experienced attacks relating to viruses, worms and/or trojans over the four-week benchmarking period → 1. Interestingly, these malicious attacks represent only around a quarter of cyber security incidents – the remainder are caused by negligence, malware or IT malfunctions.

1 The types of attack methods experienced by companies participating in the Ponemon benchmark [2]



Procedures and protocols: qualitative analysis that indicates how well-written instructions and policies secure the organization.

Cyber attacks are common, expensive and disruptive. In a survey released in 2011 of 200 IT executives in charge of oil, gas, and water utilities in 14 countries, 80 percent of them reported that they had experienced large-scale denial-of-service attacks [3]. Although mostly related to enterprise IT, these statistics indicate that any company without a well-developed cyber security strategy is risking too much in believing they will not be attacked. As cyber crime costs are, at least, two to three times higher than the cost of safeguards, proactively investing in cyber security makes good sense.

Today's control systems are more vulnerable to cyber threats than ever before due to increased interconnectivity, cloud computing and sharpened hacker skills.

Cyber attacks – the response

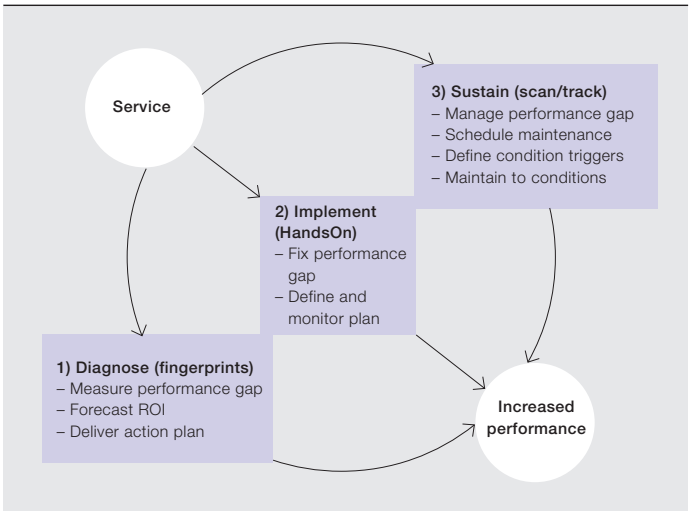
Hackers are becoming more creative and capable, and the number of such individuals and organized groups is rising, often causing damage that costs millions, if not billions, of dollars. Since Stuxnet, the malware that infected and crippled Iran's Natanz nuclear-fuel processing facility in 2010, utilities and industrial plants have been on the alert. Recently, tension has been heightened by the appearance of the "Flame" virus, the most sophisticated malicious code ever seen.

Such highly dangerous threats to control systems have caught the eye of governments, which are making moves to regulate cyber security should businesses not do so. While not necessarily bad, government-imposed regulations may miss the mark or add unnecessary cost. Moreover, a regulation-driven security approach is a poor alternative to a risk-driven one. Therefore, businesses must show they are correctly and proactively addressing cyber security, even though a 2012 Bloomberg Government study concluded that utilities, banks and other infrastructure operators may need to spend up to nine times as much as present on better security [4].

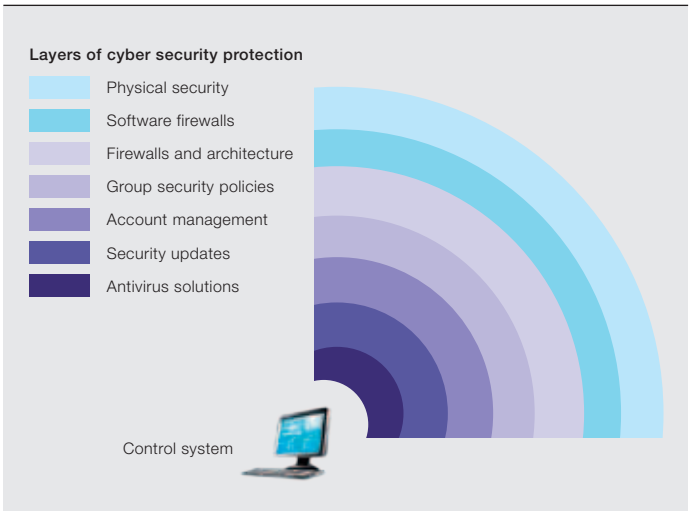
The protection challenge

Formerly, control systems were isolated from the rest of a plant's information systems. Now, business demands a much more integrated approach. Utilities and industries count on this unprecedented information sharing to gain detailed visibility into the business and to facilitate better decision-making.

2 The ABB Cyber Security Fingerprint follows ABB's proven three-step advanced services methodology.



3 Multiple layers of protection significantly reduce risk of attack



To assist customers against cyber threats, ABB created the Cyber Security Fingerprint.

Further complicating the situation is the fact that control systems tend to have long lives, up to 15 to 20 years or more. Therefore, defenses against cyber attacks may be outdated or even nonexistent. In addition, many systems include small processing devices that perform specific tasks and that are simply not equipped to run antivirus software or protective firewalls.

Furthermore, an attack on a control system can have very different consequences from one on a business system. Instead of informational and financial loss, the impact could violate regulatory requirements, damage equipment, result in production loss, harm the environment, or threaten public and employee safety.

Even though basic security measures could easily have prevented or reduced the effects of most of the intrusions described in this article, security experts are very concerned about the vulnerability of control systems to cyber attack.

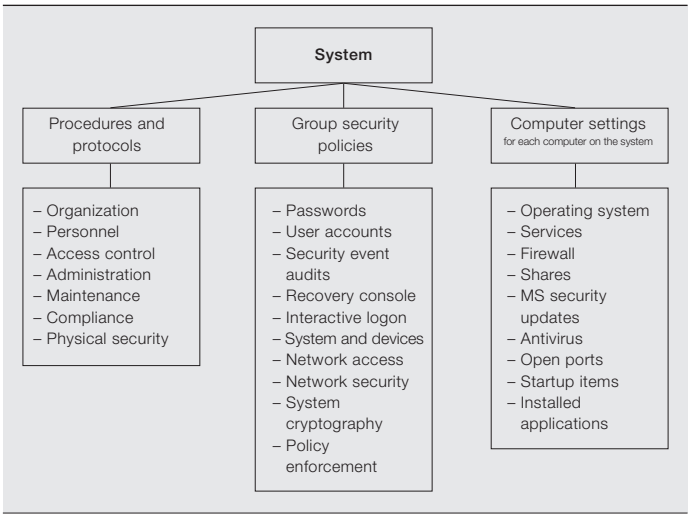
Cyber Security Fingerprint

To help customers resist cyber threats, ABB created Cyber Security Fingerprint, a noninvasive service that can be applied to most control systems running current versions of Microsoft's Windows operating system. It follows ABB's proven three-step advanced services methodology → 2. This methodology helps control system owners protect their investments and businesses by identifying vulnerabilities and outlining how best to mitigate risk:

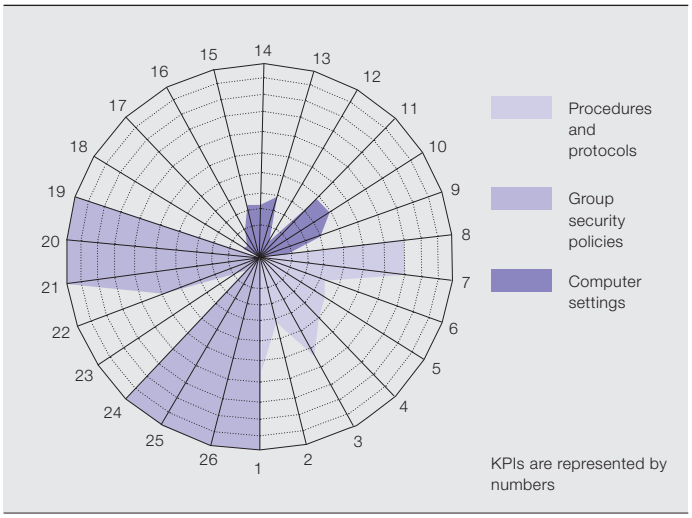
The process of identifying strengths and weaknesses, based on data gathered from critical systems and key personnel, and comparing them with industry best practices, is the backbone of ABB Cyber Security Fingerprint.

1) Diagnose: A current-state evaluation and comparison with best equipment and industry practices and standards is the first step in developing a strategy that will mitigate the risk from cyber security threats to control systems. The intention of this exercise is to identify vulnerable areas and make recommendations to address them.
2) Implement: Based on the vulnerabilities identified in step one, the physical and virtual elements of the control system are secured with the appropriate security settings, policies and procedures. This can be done by following

4 ABB examines three key components of a plant's control system to determine key performance indicators.



5 The report shows the relative risk to the system based on the assessed parts. Areas with less coloring have lower risk than those with more.



the recommendations, such as creating protocols for password settings, outlined in the fingerprint report.

3) Sustain: Ongoing condition monitoring, or at least periodic checking, is necessary to sustain a secure system in a rapidly evolving environment.

This process of identifying strengths and weaknesses, based on data gathered from critical systems and key personnel, and comparing them with industry best practices, is the backbone of ABB Cyber Security Fingerprint. ABB's approach follows the "defense in depth" principle, which means the fingerprint checks if a control system has the multiple layers of protection required to significantly reduce the risk of attack ➔ 3.

To complete the first step of the fingerprint, an ABB field engineer uses ABB's proprietary, high-speed, software-based data collection tool, Security Logger, to collect information and system settings from the control system and computers on the plant network. A temporary executable file is loaded to search all connected computers and endpoints on the customer's network and to collect profile and setting information. This process tightly follows ABB's security policies and procedures.

This data is coupled with information gathered from structured interviews with key plant personnel to compare system and plant security status with best practices and standards for the industry, such as the ISO/IEC 27000[1] series, NERC-CIP[2] and ISA-62443 (ISA-99)[3]. ABB's Security Analyzer is then used to generate key performance indicators (KPIs), which highlight strengths and weaknesses of the assessed control system cyber security ➔ 4. ABB determines KPIs for three key areas:

– Procedures and protocols: qualitative analysis that indicates how well-written instructions and policies secure the organization
– Group security policies: policies implemented on the system, enforced from a central server or implemented on individual computers
– Computer settings: settings and applications that reside on individual computers in the system

Based on the information gathered and the calculated KPIs, a diagram is generated that identifies the system's cyber security risk ➔ 5. While minimal color-

ABB's advanced service methodology helps control system owners protect their investments by identifying vulnerabilities and mitigating risk.

Footnotes

1 The ISO/IEC 27000 series (also known as the ISMS Family of Standards) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
2 NERC is an international, independent, not-for-profit organization whose mission is to ensure the reliability of the bulk power system in North America. NERC-CIP specifically applies to critical infrastructure protection (CIP).
3 ISA99 covers industrial automation and control systems whose compromise could result in any or all of the following situations: endangerment of public or employee safety; loss of public confidence; violation of regulatory requirements; loss of proprietary or confidential information; economic loss; and impact on national security.

6 Examples of findings

Subject	Description	Recommendation
Security policy	It is crucial to have a cyber security policy. The policy clearly describes what is and what is not allowed and how to react to different situations. The process of writing the policy is important because it forces the organization to discuss all aspects of cyber security.	Get managers to agree on the importance of a cyber security policy. Designate a cyber security team to write and maintain it.
Password history size	By setting a password history size, users can choose how often old passwords can be reused. Users are discouraged from cycling through a common set of passwords.	Set the password history size value greater than or equal to 13 passwords.
Windows Server 2003 SP1	Windows Server 2003 service pack 1 was introduced March 30, 2005 and the official support ended April 14, 2009.	Upgrade all server software to the latest version. NOTE: Upgrading the operating system may lead to the need to upgrade the ABB software as well. ABB's Automation Sentinel program will enable subscribers to take advantage of new ABB software and updates.

Once recommendations have been implemented, the process and tools installed enable periodic re-evaluation to measure and sustain the level of security, essential at a time when cyber attacks are evolving daily.

ation in this diagram indicates a lower risk, it does not mean the system is safe from attack. It does, however, indicate that good basic cyber security is in place for the system.

The report also includes detailed findings for each section and recommendations on how to improve vulnerable areas → 6. ABB is able to assist in implementing these. The recommendations include physical considerations, management of the entire infrastructure, policies and procedures, and governance and accountability across the organization.

Once the recommendations from the fingerprint have been implemented, the process and tools installed enable periodic re-evaluation to measure and sustain the level of security over the lifetime of the control system. This is essential at a time when cyber attacks are evolving daily.

It is important to note that the Cyber Security Fingerprint is an indicator of a system's security status at a given time. Even if all recommendations are followed, the fingerprint does not guarantee a 100 percent secure control system. No cyber security check ever can.

Comprehensive protection

The ABB Cyber Security Fingerprint is a noninvasive service that can be applied to most control systems running a current version of the Microsoft Windows operating system. It utilizes data collection, industry standards, best practices, robust technology and system security expertise to help companies protect valuable assets. Understanding control system cyber security vulnerabilities can enable utilities and industries to define and implement cyber security plans that will:

- Increase plant and community protection
- Reduce potential for system and plant disruption
- Better mitigate risk against a cyber security attack
- Lower the cost of detection, containment and recovery from cyber crimes
- Provide a solid foundation from which to build a sustainable cyber security strategy

Patrik Boo
ABB Process Automation Lifecycle Services
Westerville, OH, United States
patrik.boo@us.abb.com

Further reading

Obermeier, S., Stoeter, S., Schierholz, R., Braendle, M. Cyber security: Protecting critical infrastructure in a changing world. *ABB Review* 3/2012, 64–69.

References

[1] Ahlers, M. (2011, November 18). Feds investigating Illinois 'pump failure' as possible cyber attack. CNN.com. Retrieved July 10, 2012 from http://articles.cnn.com/2011-11-18/us/us_cyber-attack-investigation_1_cyber-attack-cyber-security-national-cybersecurity?_s=PM:US
[2] Ponemon Institute. (August 2011). Second annual cost of cyber crime study: Benchmark study of U.S. companies. Traverse City, MI.
[3] Torrenzano, R., Davis, M. (2011). Digital Assassination. New York; St. Martin's Press.
[4] Engleman, E., Strohm, C. (2012, January 31). Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps. Bloomberg.com. Retrieved July 10, 2012 from http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html