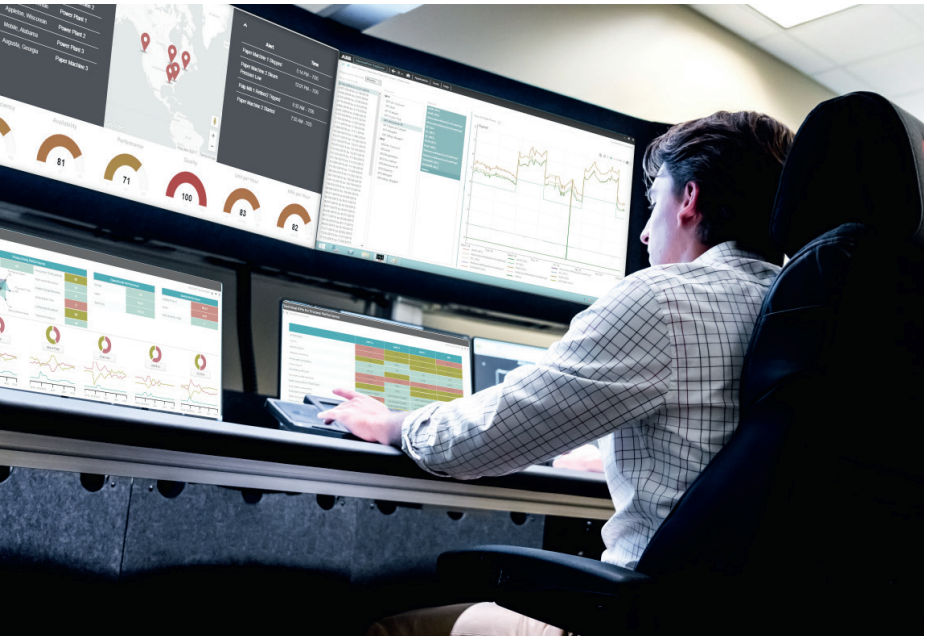
THOUGHT LEADERSHIP

Pay attention: Don’t get caught without a cyber security strategy



01 Industrial control systems are increasingly coming under attack by common viruses aimed at Windows operating systems.

The need for a solid cyber security strategy has been discussed and debated for 50 years and yet the basic worm-type attacks first documented in 1972 are still with us today. Why? Because even the most basic measures to protect control systems from these types of attacks are still not systematically employed.

It’s hard to believe there are still thousands of systems in operation today without any basic security controls in place. If you own a car, a house, or a boat — just about any “big-ticket” item that would be expensive to replace — you protect that asset with insurance. Even though you can’t see it or feel it, you know, instinctively, it’s worth the money. You sleep better at night knowing you have it and it would be a high priority item to reacquire if you lost it — especially if it contributed to your livelihood. But, when it comes to control system cyber security, this thinking, for some reason, often is not applied. Cyber experts are still struggling to convince senior management to spend money to protect their control system assets.

Recent events should be setting off alarm bells in board rooms across the industrial world. Two viruses, WannaCry and NotPetya, have wreaked havoc on companies that were running older Microsoft Windows operating systems but failed an entry-level cyber security test: keep your systems patched and up to date.

—
02 Screenshot of the Petya ransomware, a cousin of NotPetya and WannaCry.
—
03 Attackers often look for a return on their investment in the form of a ransom, but not always. Some attackers simply seek to disrupt and destroy critical control systems.

—
02

Both of these viruses were destructive. WannaCry was standard ransomware, but NotPetya was a wiper bug masquerading as ransomware. Its purpose: cause maximum damage to the systems it infected. It forced thousands of large complex operations in many industries to halt production by scrambling data and offered no way out (such as paying for the decryption keys) to its victims.

ATTACKER OBJECTIVES

LOSS	• Loss of View • Loss of Control
DENIAL	• Denial of View • Denial of Control • Denial of Safety
MANIPULATION	• Manipulation of View • Manipulation of Control • Manipulation of Sensors and Instruments • Manipulation of Safety

—
03

Impacted companies have disclosed the financial impact of these attacks. It's not pretty:

- One of the world's largest container shipping companies, with substantial oil and gas assets as well, wiped as much as $300 million off its books in the third quarter of 2017
- A skin-cream maker lost $41.5 million in first-half sales
- A French building materials manufacturer said it lost about $280 million in sales in 2017
- The worldwide pharmaceutical production of a major drug producer was disrupted to the tune of $670 million in 2017
- A major international package delivery company announced a loss of $400 million

That is a lot of money — over $1 billion in total — money that could have refreshed legacy systems, acquired new assets, invested in R&D, paid employee bonuses, delivered stockholder dividends, etc. Certainly some of it should have been spent hardening these organizations' systems against such events. So why wasn't it?

Why companies don't invest in cyber security
Part of the answer is pretty simple: it's hard to convince companies to spend money on something that has no measureable return on investment (ROI). Basically, it's hard to put a dollar value on an event that may not happen.

Of course, everyone knows cyber security is important and falls into the general category of risk management. But, as an event such as the massive oil spill in Alaska's Prince William Sound in 1989 proves, the cost of doing nothing is far greater than the cost of being proactive (super tankers are now made with double hulls to prevent a repeat of that ecological disaster).

It isn't that control system owners don't deploy cyber and security solutions; they do. They are aware of the problem and take actions to avoid risks. But many in the industrial world are still too focused on the big attack or hack — the nation state that blacks out an entire region or shuts down the water supply to a city — when the bigger and more likely risk is common malware that impacts a control system because it is running older, unprotected and unpatched operating systems.

This risk exists even if the system is "air-gapped" from the business's network. People often introduce data and software from removable media such as USB drives, exposing their systems to the potential for viruses along the way. As these air-gapped systems

become more interconnected to enable integration with business applications, they become increasingly exposed to the internet. As we've seen in the past with WannaCry and NotPetya, this is why it is far more likely common malware will cause the most damage in the long run.

This is because there is a fundamental disconnect in securing operational technology (OT) vs. information technology (IT). But, as OT becomes more exposed to the internet, it faces the same cyber security threats as any other networked system. This is because operators have adopted the same hardware, software, networking protocols and operating systems that run and connect everyday business technologies, such as servers, PCs and networking gear.

At the same time, many machines and legacy systems are so old and proprietary, no self-respecting cyber-criminal would ever write malware to attack them. Why? There just aren't enough of these systems around to make it profitable (typically the main motive of hackers everywhere today) or notorious (if they have more harmful motives).

That leaves control system operators in a tough position. If they try to deploy the same security measures as IT then a) they may not work or b) IT security measures, when effective, may actually shut down a running production process. This could be more harmful for the business than the cyber-attack.

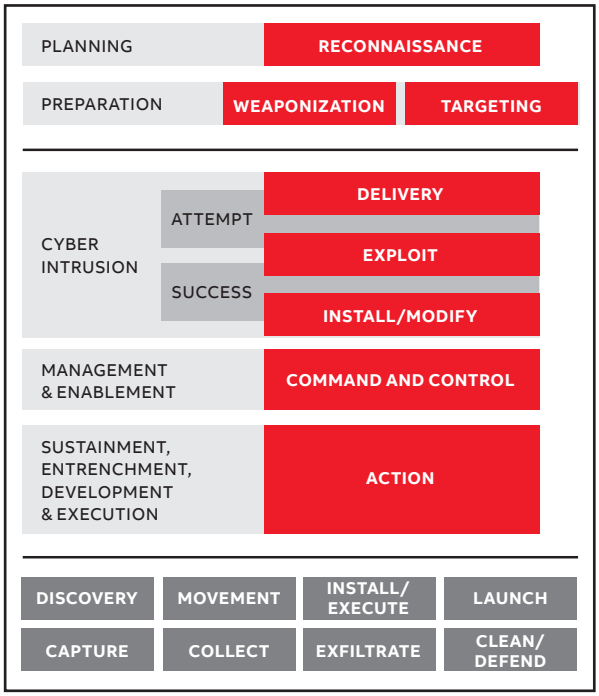
The problem is that IT cyber security solutions tend to focus on locking down data when there is a threat. That makes sense if it's a credit card database, but it doesn't work so well if a firewall blocks programmable logic controllers (PLCs) from opening and closing valves in an oil refinery or pulp mill.

Luck is not a strategy

And then there is just human nature. Many operators simply rely on wishful thinking that goes something like this: "We haven't had an incident, therefore, we must be doing the right things." Well, not really. If you assume not having been attacked or hacked means you are doing enough, think again. You could just be lucky. Being lucky is great, but you should not rely on luck as a strategy. Talk to a professional gambler and they will tell you eventually luck runs out.

STAGE 1

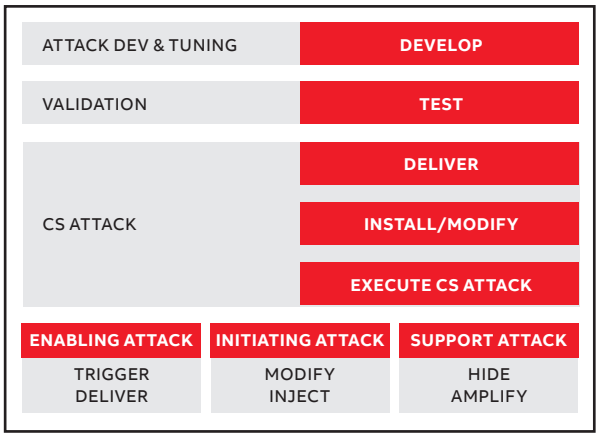
CYBER INTRUSION PREPARATION AND EXECUTION



—
04

STAGE 2

CONTROL SYSTEM (CS) ATTACK DEVELOPMENT AND EXECUTION



—
05

—
04 Cyber-attacks today are not random. They are sophisticated, planned, and executed with intent. Stage 1 is preparation. It mimics a targeted and structured attack campaign.
—
05 Stage 2 is execution. It shows the steps associated with a material attack that requires high confidence.

So, how do you know the difference between luck and "Doing the right things?" Ask yourselves the following questions. If you answer "no" or "don't know," then perhaps you should consider yourselves "lucky" and start taking a hard look at your cyber security posture and policies:

1. Do you regularly train your employees on cyber security best practices?
2. Do you have a comprehensive list of cyber assets?
3. Have you performed an operational risk assessment?
4. Have you performed a cyber security assessment?
5. Have you implemented proper network segmentation?
6. Have you implemented end-point malware prevention and do you update the signatures on a daily basis?
7. Do you patch your systems on a regular basis (minimum quarterly, ideally monthly)?
8. Are you monitoring your system logs and network traffic?
9. Do you have a backup of all your assets, such as switches, routers, firewalls, programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs) and every other digital control asset with a configuration file?
10. If your system were compromised today, do you have a recovery and response plan ready?

If you answered "no" to one or more of these questions, you are not alone. Most control system owners do not employ this level of cyber security readiness. But, at a base level, if you do not have proper network segmentation, updated system software, end-point protection and hardened systems, then you are probably lucky that your system hasn't been compromised.

Getting up to cyber speed

When thinking about how to get started, don't just look for some new technology that claims to mitigate all your risks — it doesn't exist. Doing the basics well before investing in advanced cyber technologies is the key. In order to minimize your risks and get the most protection in the least amount of time, you first need to plan and develop a cyber security program that:

1. Identifies what assets you are trying to protect
2. Determines how you are going to protect those assets
3. Enables intrusion detection and monitoring
4. Defines incident response processes and procedures
5. Verifies mechanisms to restore and recover assets
6. Ensures compliance with all regulatory standards set by local governing bodies

These six steps follow well-trodden ground. All cyber security best practices frameworks can be distilled into these basic steps: identify, protect, detect, respond, recover and comply.

For example, putting in a firewall to separate your control system from the corporate/business network is a great idea. But, if you don't have an inventory of critical assets and applications, you may still be vulnerable to risks from employees and contractors who use laptops and removable media. Developing strong security policies and practices, and mapping out a three to five year journey that leads to security maturity is also highly recommended.

Some effective technology tactics to consider are hardened perimeters, adopting a defense-in-depth approach, whitelisting, investing in network intrusion prevention (IPS), air-gapping control system and security awareness training for all employees. Also, make sure to include specific contractual language about cyber security in your OT/control system requests for proposals (RFPs). To execute your plan, leverage your IT and OT teams, but also look for OT suppliers who can offer comprehensive cyber security services.

Conclusion

The list of things you should do to protect your operational technology is long and beyond the scope of this paper, but if you continue to do nothing, imagining that your systems are safe from attack, it is only a matter of time before you won't be imagining. Eventually, your luck will run out. Don't let it be your systems that go down this time, or your company that ends up in the headlines.

—

ABB Inc.
579 Executive Campus Drive
Westerville, OH 43082
Phone: +1 800 435 7365

abb.com/cybersecurity

9AKK107202