# The path to Cyber-Security

**William Aja, Vice President of customer operations for Panacea Technologies Inc**

*Hello seminar attendees!*

*I hope you are all enjoying the ISA-France seminar. As it has been since the beginning of our industry, everything seems to be changing. As various control disciplines merge, and responsibilities grow, it is apparent that a great shift in focus has happened. The Internet of Things, cloud operations, and all things "cyber" have gripped our industry. Most conferences and industry publications have large focus on cyber-everything and I suspect it is only the beginning.*

*I ask one thing of you though, which is to remember that it is all of our collective responsibilities to keep our infrastructures secure. Whether you realize it or not, we all have a duty to protect our manufacturing plants and industrial infrastructures. We also have a duty to ensure the innovation that drives us isn't extinguished by fear, uncertainty, and doubt of the unknown. Cyber-security is a multi-faceted solution to an ever-changing threat, but the basis of security begins with all of us.*

Cyber-security is becoming a big problem for modern manufacturers. At an ISA conference a few years ago I remember hearing a panel discussion where an expert was asked why we didn't see more cyber-attacks on manufacturers. The expert responded "hackers probably don't know where to look; most people don't even know what a PLC is".

Although there is some truth to this, another reason is that, until recently, automation infrastructure was safe by design. Cyber-attacks rely on a lot of factors for success, but they penetrate your defenses through an Attack Surface. An Attack Surface is a way to describe the entire canvas which an attack is capable of penetrating and infecting. Imagine your plant like a house, and cyber-attacks are just burglars trying to get at your prized possessions. Windows, doors, garages, etc. are all Attack Surfaces that need to be defended.

Traditionally control systems had very small Attack Surfaces due to their network design. This was because computers and server infrastructures sat segregated behind firewalls and connected devices and I/O networks were shielded from attack.

As more functionality is demanded out of control systems, this architecture has evolved introducing new functionality, but has also increased the Attack Surface. In some cases the larger Attack Surface is easily identifiable in the form of expanding computer and server infrastructures, applications that require enterprise connectivity, and un-managed laptops used for trouble shooting and code changes. In some cases the Attack Surface grows in ways that aren't immediately obvious in the form of smart coffee makers, IIOT devices residing at the IO layer, security cameras, telemetry devices etc. Although the main control network may sit behind a firewall, these devices often have their own connection to the enterprise network.

This may seem farfetched, but we've already seen assaults on these new Attack Surfaces. In June there was a report that a smart coffee machine became infected with a malware attack that spread from the coffee machine to several outdated Windows machines on the control network shutting down the plant. In late July ICS-CERT issued a report of vulnerabilities on a well-known telemetry device that caused it to transmit fraudulent data and unleash DDOS attacks meant to cripple internal networks. Earlier in the year an attack called "Crash Override" was discovered that could map out industrial networks, and then unleash an attack on vulnerable smart devices. It activated on its own and took down an entire Eastern-European power grid. Late last year we saw a record breaking DDoS attack that was orchestrated using internet security cameras.

The point is that as we demand more functionality and connected features out of our control systems; we are increasing our risk for attack. The solution is not to abandon these features in favor of security, or disconnect from the enterprise all together (a method that proved ineffective against *WannaCry* and *NotPetya* attacks anyways) but rather design systems to minimize the potential Attack Surfaces and create a robust and constantly evolving defense strategy to protect those Attack Surfaces.

One of the most critical pillars of all cyber-security plans must be patch management. Staying up to date on the latest OS and application patches ensures your infrastructure receives critical security updates meant to eliminate vulnerabilities. Unfortunately we see clients adopt one of two, equally flawed, patching strategies that leads to exposed Attack Surfaces and frustrated staff.

The first method is the "deploy all patches" method which deploys patches that aren't automation vendor tested or approved, breaking automation systems and causing data quality issues and downtime events. Burnt by the results of this method, manufacturers may then adopt the "deploy no patches" method which ensures downtime events from unapproved patches are eliminated but critical security updates are not deployed either. Networks are often air gapped as a way to remediate this problem, but even air gapped and segregated networks can be infected as seen by the most recent malware attacks.

Internally Panacea recognized this need a long time ago and we have been working with our clients to implement minimized Attack Surface designs and have developed novel security platforms such as the Panacea Update Manager. It manages Microsoft patches for automation systems and ensures that only vendor tested and approved patches are deployed onto your Industrial Control Networks. We utilize this tool to manage our internal computer infrastructure and it is available for manufacturers to deploy internally as well.

We in the automation community need to recognize that it is a collective social responsibility to protect our manufacturing plants that make so many products essential to our modern society. The path to a fully-fledged cyber-security plan can seem overwhelming, but by simply decreasing Attack Surfaces and having robust security methodologies in place you will be well on your way to a safer more secure plant.

## About the Author

**William Aja** (ajaw@panaceatech.com) is Vice President of customer operations for Panacea Technologies Inc, He has a passion for automation and process control, and focuses on delivering automation services ranging from cyber-security and IIoT consultation and feasibility studies to turnkey process control solutions and long term service and support. Panacea Technologies Inc (http://panaceatech.com) is a member of the Control System Integrators Association (CSIA) (www.controlsys.org).