ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Hacker's Paradise: What It Takes to Achieve a Secure Connected Factory

Erik Halthen, Systems Manager for Industrial Solutions

Which Would You Choose? A $30 Million Ransom or Disrupting Your Organizational Structure?

You're the CIO of a manufacturer. Your production line is running along smoothly when, suddenly, the lights go out. The backup generators kick on and the factory floor is dimly lit by the emergency lights. What happened? Your IT manager calls to let you know that he received the hacker's email informing him that your factory has been hit by a ransomware attack. Several areas of your business are paralyzed, and you are faced with two choices: pay the hacker's ransom or try restoring your system via your backup files. You decide to use your backup files, which in the end cost you $30M in lost production revenue and downtime.

Are you ready to pay cyber hackers hundreds of thousands, if not millions of dollars to unlock your files? According to the January 23, 2019 State of Malware report provided by Malwarebytes Labs:

"Malware authors pivoted in the second half of 2018 to target organizations over consumers, recognizing that the bigger payoff was in making victims out of businesses instead of individuals. Overall business detections of malware rose significantly over the last year—79%to be exact—and primarily due to the increase in backdoors, miners, spyware, and information stealers."

How did this scenario happen? The digital age continues to open new doors of possibility. Business leaders are finding new opportunities to innovate, but this innovation comes with challenges. Addressing cyber security risk is one of the most significant challenges faced by business leaders, and it requires unconventional changes in organizational structure. These changes are required to effectively instill the organizational culture and the adoption of new business processes to address system and lifecycle complexity.

The rapid adoption of new smart edge devices that create and interpret data is responsible for the exponential growth in complexity. This data has value because decisions are made from the data, and the more precise and accurate the data, the higher its value. But realizing this value is complex. It requires an infrastructure capable of accessing and interpreting the data in a timely manner, to allow for decisions to be made in a relevant elapse of time. This need is driving the connected world and, in terms of industrial automation, the connected factory. Devices must be interconnected on a distributed network to enable the creation of value through the timely access and interpretation of data.

The megatrend, known as Industry 4.0 is opening new opportunities for innovation as factory control systems become more agile, more accurate, and more efficient. Addressing the risk of cyber attacks and ensuring the validity of the data and subsequent decisions are paramount to enabling valuable outcomes of the connected factory. As the incentive to perform cyber attacks continues to grow in proportion to the value of the assets, addressing the risk is no simple task. Considering the complexity of cyber security and the need to address the cyber security risk at a system level, business leaders are looking for guidance.

The guidance is found in terms of new security standards by governing bodies such as the International Society of Automation (ISA) and the National Institute of Standards and Technology (NIST). Although regions may adopt different variants of standards, these standards are relatively constant with each other. However, standards are only part of the solution to this complex problem. They provide guidance on how to assess risk and what methods can be used to guard against risk. To successfully implement a secure connected factory, a top down organizational shakeup is required.

Implementing a secure connected factory requires an organization capable of interpreting standards and building security infrastructure. The interpretation of security standards to proportionately address cyber risk results in security requirements. The development of critical security infrastructure is necessary to manage assets throughout the product lifecycle for a constantly changing threat environment. Ushering in the new connected age starts with building an organization capable of driving business processes from the top down. This will enable product development teams to assess security trade-offs and formulate product security requirements that address system and lifecycle complexity.

The Unseen Challenge to Securing the Connected Factory

Applying security to a complex, operational technology (OT) environment presents unique challenges that cannot be addressed with standard informational technology (IT) solutions. OT devices exist in an environment of competing asset values, priorities, and constraints that differ from the IT environment. In the IT environment, there is a significant bias toward ensuring confidentiality; whereas, on the factory floor, availability of data often becomes the highest priority. Additionally, the security solution will exist in a system with highly constrained products and lifecycles spanning greater than 20 years. Making sense of the factory assets, priorities, and constraints requires a unique set of skills and processes to develop adequate product security requirements. These skills and processes often exceed the capabilities of the traditional IT organization.

Figure 1. Threat modeling process.

Securing the OT environment is a system approach that requires identifying high value assets, assessing the risk to those assets, and making appropriate security trade-offs within its concept of operations. Because of highly constrained environments and unique operational designs, not all the security risk will be addressed at the device level. A defined system-level approach will guide experts to make appropriate security trade-offs. There are many ways to perform threat modeling, but organizations must adopt a process for all new development.

The primary goal of threat modeling is to drive a discussion around security trade-offs to finalize security requirements and specifications. To do this, a concept of operations will serve as a basis for identifying critical assets and decomposing a system. Once this exists, the team can start identifying threats and vulnerabilities using establish methodologies, which will serve as the preliminary threat model. Using this model, security mitigations can be established, and trade-off discussions should occur. Since the concept of operations should consider the entire system design, it is critical to ensure all appropriate stakeholders are involved in any trade-off discussion. Ultimately, any security threat not addressed at a component level must be mitigated at a higher level or accepted as a tolerable risk. Adopting a standard process to engage in threat modeling and risk analysis will help ensure adequate security requirements are derived.

Organizational Rise to Enabling the Connected Factory

The cyber security threat on the OT requires organizations to strategize on an approach to enabling the connected factory. Successfully addressing the complexity of the cyber security threat often requires organizational change. Having a security expert as part of a product team is a step in the right direction, but it is not enough to enable an organization to successfully capitalize on the next industrial revolution. To do this, the change must occur at the highest levels of an organization with sponsorship to drive and enable a cultural change that will extend through the entire business enterprise. This means a central organization for cyber security that will implement new processes and procedures to assess cyber risk, apply cyber security requirements, monitor and respond to cyber security incidents, and perform product assessments and validation.

The formation of a product security assurance program is critical to address future cyber security risk. This program will ensure development teams understand the cyber security risk, the critical assets to protect, and the security functionality required to drive operational performance. The people and processes to support this program must be in place to ensure cyber security is addressed throughout product lifecycles and to establish a resilient infrastructure for enabling quick response to new cyber security threats and incidents.

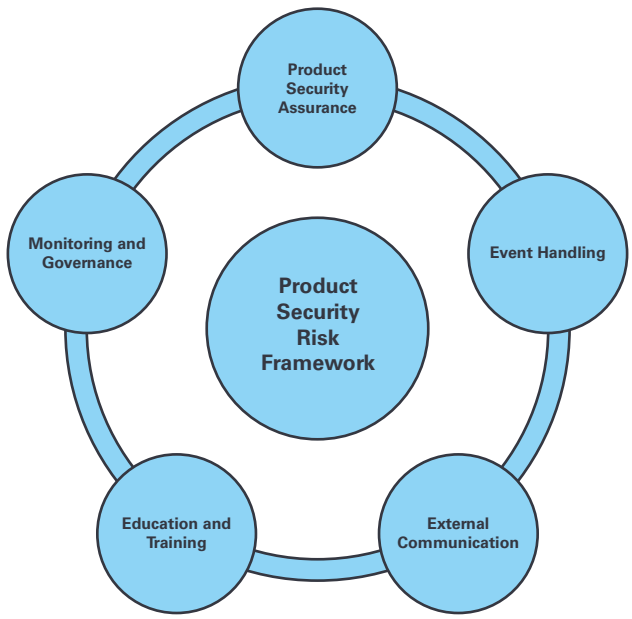

Figure 2. Product security risk management framework.

Organizations will need to respond to new cyber security requirements by demonstrating an awareness and approach that is routed in organizational culture and driven by standard processes and procedures. The organizational aspect to addressing the cyber security risk is the most difficult part of transitioning to the connected factory. All companies will need to respond to this challenge, and those leading the cultural change are in a better position to capitalize on one of the most significant megatrends of our time.

Analog Devices has responded to the changing cyber security environment by establishing a central security group responsible for fostering a security culture throughout the organization. Releasing security processes that are integrated with the new product development processes is a critical step to driving the security culture throughout the organization. This ensures all new products are evaluated for security needs and a security advocate is assigned to the development. The security advocate is responsible for ensuring security requirements adequately protect critical assets as they exist within a fully integrated system design. Since security is always a matter of making appropriate trade-offs, Analog Devices' security implementations are validated with lead customers responsible for the security of the connected factory. Validating our security implementation with customer stakeholders ensures security trade-offs are made that enable the operational environment.

As part of institutionalizing a security culture, Analog Devices' champions a cyber security incident response team to assess new security threats, respond to customer cyber security incidents, assess product impact, and drive product security updates. The long-term impact to managing a vast portfolio of products can be substantial. Appropriate planning takes place to promote sustainability and management of our security solutions across the entire product portfolio. As system integrators turn to their supply base to solve the tough security challenges and reduce total lifecycle cost, new product selection criteria will result in strong partnerships to manage the total cost of the connected factory. Analog Devices is committed to the long-term solution that provides the best overall value to new system designs.

If the choice is organization disruption or accepting risk, one should choose organizational disruption over paying a ransom any day.

References

Kujawa, Adam, Wendy Zamora, Jovi Umawing, Jerome Segura, William Tsing, Pieter Arntz, and Chris Boyd. "2019 State of Malware". Malwarebytes, January 2019.

About the Author

Erik Halthen, part of ADI's acquisition of Sypris Electronics in 2016, brings an extensive background in cyber security solutions. As part of ADI's cyber security center of excellence, Erik has taken on the role of security systems manager for industrial solutions. Leveraging his experience as a cyber security program manager in the defense industry, Erik is focused on developing leading security solutions to meet key market demands in Industrial IoT He can be reached at *erik.halthen@analog.com*.

Online Support Community

ADI EngineerZone™
SUPPORT COMMUNITY

Engage with the Analog Devices technology experts in our online support community. Ask your tough design questions, browse FAQs, or join a conversation.

Visit *ez.analog.com*

T21614-10/19

For regional headquarters, sales, and distributors or to contact customer service and technical support, visit analog.com/contact.

Ask our ADI technology experts tough questions, browse FAQs, or join a conversation at the EngineerZone Online Support Community. Visit ez.analog.com.

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

VISIT ANALOG.COM