CYBERSECURITY CONSIDERATIONS FOR YOUR SMB

Small to medium-sized businesses are implementing IIoT technologies at a breakneck pace. While this adoption is key to your business success, don't overlook the cybersecurity risks inherent in an ever-connected world.

Mike Watkins,
Business Development

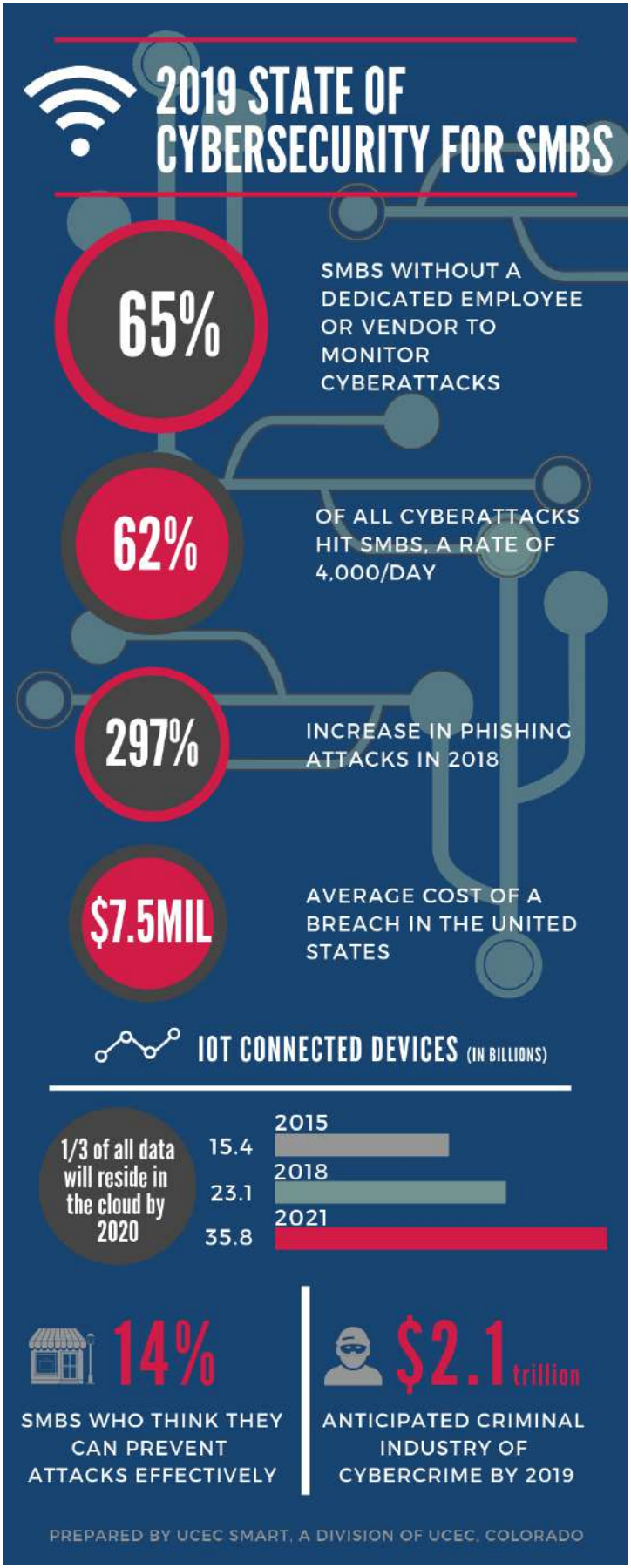
Rapid IIoT Adoption

Executive Summary

A robust industrial control systems (ICS) cybersecurity posture requires sufficient funding for technologies, managed security services, and trained IT personnel. Based on the graduate course study on the Internet of Things at Colorado University and the research presented here, the best solution for small to medium-sized businesses (SMBs) may be a "minimum viable product" approach.

Extensive adoption of the Industrial Internet of Things (IIoT) could generate significant economic gains for multiple industries. Accenture estimates that IIoT might add $14.2 trillion to the world's economy by 2030. This is entirely plausible because sensors are extremely affordable, and tens of billions have already been implemented in IIoT to improve productivity and reduce operational costs.

Small to medium-sized businesses (SMBs) are implementing IIoT technologies at a rate that oftentimes exceeds the rates seen at the enterprise level. The Nationwide [Insurance] fourth annual business owner survey, released in September 2018, surveyed 1,000 small and mid-sized business owners about their views on cybersecurity and found that an overwhelming majority – 91 percent – used connected technology. But 48 percent of those surveyed were "unconcerned" that devices – ranging from sensors to drones and used across any number of verticals – may boost their likelihood of cyberattacks.[1]



Tim Nunziata, Director of E&S Specialty at Nationwide, described the use of drones in agriculture to illustrate the scope of the problem. According to Nunziata, the American Farm Bureau has estimated that roughly 75 percent of commercial farmers have IIoT technologies in place, but less than 5 percent have plans in place to deal with breaches.[2] In most instances, there is no one within the SMB tasked with protecting industrial control systems. In fact, the Nationwide survey found that 65 percent of SMBs do not have a dedicated employee or vendor in place to monitor cyberattacks. Going forward, however, it is clear that SMBs will need to identify internal or external resources that are familiar with the state of ICS cybersecurity; that are conversant in the basic best practices of industrial cybersecurity; and, that are staying abreast of the rapidly changing landscape of ICS threats.

The impact of the Internet of Things

IoT [IIoT] and data statistics are staggering, to the point of appearing fantastical[3]:

•5 quintillion bytes of data produced every day (that's 2.5 followed by 18 zeros)

•By the year 2020, the IoT will comprise more than 30 billion connected devices

•It would take a lifetime to manually analyze the data produced by a single sensor on a manufacturing assembly line

No wonder studies reveal that:

•Only 26% of companies surveyed reported that their IoT initiatives have been successful

Despite the fact that statistically the chance of success are woeful, small to mid-sized businesses will have to press on because SMBs that are not taking advantage of IIoT will be left behind. As a result, the number SMBs that are not taking the steps necessary to secure their systems is worrisome.

Although larger companies – companies with more than 100 employees – comprise only 1.83% of all US companies, they employ 66.29% (two thirds) of the workforce and generate 75.78% (three quarters) of the gross domestic product (GDP). The take-away is, despite the fact that 98.17% of companies have less than 100 employees, the 1.83% of companies with more than 100 employees employ twice as many employees and generate three times more revenue. These statistics explain why SMBs historically have not received the attention of solutions providers – the perceived ROI is just not there.

To provide context to the scope of the problem, the U.S. Census Bureau, *Statistics of US Businesses* (2014) reports that 89.36% of all US businesses employ less than 20 employees, and 98.17% of all US businesses employ less than 100 employees.

	<20 empls	<100 empls	>100 empls
Businesses	89.36%	98.17%	1.83%
Employees	17.08%	33.71%	66.29%
Revenues	12.24%	24.33%	75.78%

U.S. Census Bureau, *Statistics of US Businesses (2014)*

62% of all cyber-attacks hit SMBs, but most small to medium enterprises are not adequately prepared[4].

As mentioned in the opening, the traditional SCADA systems in use by SMB manufacturers, et al., have several challenges when it comes to security. With more data being transported than ever before, it will be important not only for them to secure their physical assets, but to secure their communication links as well. Traditionally, SCADA systems have been on the outside of a firewall from the corporate IT network. Newer SCADA systems will require more crossover between IT and OT systems and, therefore, should employ Ethernet devices that are more security-focused alongside measures such as VPN, secure sockets, encryption and dedicated log-ins on the devices.

Data is the "blood" flowing through IIoT systems9, and the sheer number of "blood-born" diseases that might flow through an IIoT system are absolutely staggering. For example, sensor data may be tampered with, stolen, deleted, dropped, or transmitted insecurely, allowing it to be accessed by unauthorized parties. IIoT devices may be counterfeited, and default credentials used. Furthermore, unlike traditional personal computers, there are few security upgrade processes for IIoT devices such as patches or updates.

DATA POINTS

- In 2018, we have seen a 350% increase in ransomware attacks, a 250% increase in spoofing or business email compromise (BEC) attacks and a 70% increase in spear-phishing attacks[5]
- Small and mid-sized businesses are hit by 62% of all cyber-attacks or about 4,000 per day, according to IBM[6]
- Attackers focus on SMBs because they have comprehensive client data and unprotected systems
- Only 14% of small businesses consider they can manage or prevent attacks effectively
- According to the U.S. Securities and Exchange Commission, the average cost of a cyber-data breach has risen from $4.9 million in 2017 to $7.5 million in 2018
- A recent report from Cybersecurity Ventures predicts ransomware damages will cost the world $5 billion in 2017, up from $325M in 2015 – a 115X increase in just two years!
- According to the same source, global damage costs in connection with ransomware attacks are predicted to reach $11.5 billion annually by 2019
- At some points, the average IoT device was attacked once every two minutes! The most significant weakness? A default password[7]
- Cybersecurity Ventures predicts there will be a ransomware attack on businesses every 14 seconds by the end of 2019. This does not include attacks on individuals, which occurs even more frequently
- Employee negligence resulting in breaches, increased by 48% over the previous year [2017 to 2018]. In 2018, one-third of the SMBs could not determine what allowed attackers access to system data[8]

I would be ideal if there was an IIoT cyber security standard to which all companies could adhere to. Although there isn't such a standard, much is being done to establish one for our nation's critical infrastructure. For example, in April of this year, The National Institute of Standards and Technology (NIST) issued the "Framework for Improving Critical Infrastructure Cybersecurity". The document is the result of a collaboration of private- and public-sector individuals and organizations, and provides a cybersecurity risk framework for voluntary use by critical infrastructure owners and operators.

Alongside the NIST effort, there are the efforts of the Department of Energy (DOE), Federal Energy Regulatory Commission (FERC), which is the federal authority tasked with overseeing the reliability of the nation's power grid. As part of their charter, they were given the authority to approve mandatory cybersecurity reliability standards. These mandatory standards have gone a long way towards the rapid adoption of robust cyber security best practices at power plants across the country. As recently as April 2018, FERC issued the "Final Rule on Critical Infrastructure Protection Reliability Standard CIP-003-7 (Cyber Security and Security Management Controls) Order No. 843", which further cemented the standards.

"Much is being done to create an IIoT cyber security standard for our nation's critical infrastructure"

In recent years, private entities and consortiums have come together to establish non-mandatory standards for companies that are not involved in maintaining our nation's critical infrastructure. For example, the Industrial Internet Consortium (IIC) has taken the position that cyber-security is a threat that does not discriminate, and represents a major threat to world safety and security. They feel that enterprises large and small are at risk of being attacked from unexpected sources both inside and outside the system, whether intended or accidental. The Consortium is made up of an august collection of firms – including AT&T, Intel Corp, Johns Hopkins University, Microsoft and Symantec – and they believe that addressing this cyber-security challenge is critical to the success of IIoT and the Industrial Internet revolution.

IIC members were very ambitious as they set out to initiate a process to create broad industry consensus on how to secure IIoT systems. The members acknowledged that IIoT is being shaped by many participants from the energy, healthcare, manufacturing, transportation and public sectors, each with specific, and sometimes unique, security considerations. As a result, the members sought to build early consensus in the development of a common security framework. The document – "Industrial Internet of Things, Volume G4: Security Framework" – represents an urgent and important attempt to codify an approach for avoiding security hazards, especially as systems from different sectors interoperate and exploitation attempts are made in the gaps between them.

Alongside the IIC effort, there is the American National Standards Institute (ANSI) / International Society for Automation (ISA)/IEC 62443 series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). The guidance in the standards are intended to apply to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, implementing, or managing IACS.

Note that these documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

The ISA Security Compliance Institute (ISCI) created the first conformity assessment scheme (commonly known as a certification scheme) for the ISA S99 IACS cybersecurity standards. This program certifies Commercial Off-the-shelf (COTS) IACS products and systems, and addresses securing the IACS supply chain. ISCI development processes include maintenance policies to ensure that the ISASecure® certifications remain in alignment with the IEC 62443 standards as they evolve. While the IEC 62443 standards are designed to horizontally address technical cybersecurity requirements of a cross-section of industries, the ISASecure scheme's certification requirements working groups include subject matter experts from the chemical and oil and gas industries and are reflective of their cybersecurity needs.

The ISASecure® scheme requires that all test tools be evaluated and approved to ensure the tools meet the functional requirements necessary and sufficient to execute all required product tests and that test results will be consistent among the recognized tools.

The Minimum Viable Product Solution

Most SMBs do not have the internal knowledge or experience necessary to make the IT – OT connection, successfully implement an IIC security framework, or receive ANSI/ISA-99 certification. As a result, SMBs that are beginning to investigate the value associated with implementing IIoT should be exploring alternative cybersecurity strategies. One viable alternative would be to work with hardware manufacturers, software vendors, network providers and technology integrators to ensure that their IIoT devices and systems work securely together to realize their full value. In fact, a really good approach for diverting an SMB cyber security disaster would be to encourage SMBs to source integrators that can design for them an IIoT "minimum viable product" (MVP).

Five Components Addressed by the MVP

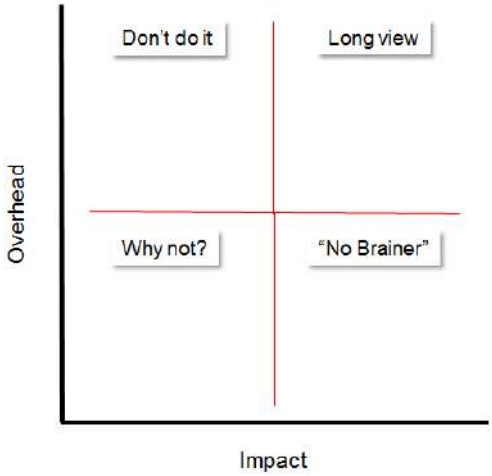
1. A hardware device (sensor)
2. A device unique identifier or IP (Internet Protocol) address
3. Internet connectivity and encryption
4. Software and cloud platform
5. The platform integrator

Since standardization of IIoT is still a long way off, the current way forward would be to develop partnerships and ecosystems for proper authentication and authorization of devices and systems, especially due to heterogeneity of the devices and systems in the network. Fortunately, there are technology providers available that are security focused and will help to provide the extra layers of security required to bridge OT and IT networks. The role of the SMB is to adapt a business focused, risk-based approach to IIoT cybersecurity. Organizations with a cybersecurity framework that is consistent and at least fairly rigorous shall be well equipped to work with a third party to formulate a plan to reduce their cyber risk.

Of course the resource and maintenance overhead needs to be weighed against the potential financial impact of security breaches. On the one hand, Juniper Research has predicted the total cost of data breaches will soar to $2.1 trillion globally by 2019 – almost four times the estimated cost of breaches in 2015. On the other hand, the average SMB has considerably less at risk. The challenge is to come up with a strategic plan for how to achieve the biggest risk reduction "bang for the buck".

Risk reduction is the "bang", and it is synonymous with "Impact" in the four quadrant model to the right. Invested resources are the "buck", and they are synonymous with "Overhead" in the model.

If pursuing an IIoT strategy places the SMB infrastructure at high risk, then the cybersecurity solution will need to be a really impactful one. The organization will need to find a low cost (overhead) solution that has high impact (robust cybersecurity) – which is a "no brainer" to proceed with. Absent a low cost solution, they would need to find a higher cost solution that provides the same robustness – a "long view".



The "no brainer" is an easy decision for the SMB to make. The "long view", not so much. When the "long view" is the only option, many SMBs will select a low cost (overhead) solution that has very little impact (weak cybersecurity). They adopt a "why not?" or "what have we go to lose" posture to their modest investment. The result will be to subject high risk infrastructure to bad actors that easily penetrate unprotected assets.

The "low hanging fruit" to be mined in the low cost / high impact quadrant may come in the form of quality routers and smart devices. Routers are the IIoT devices that suffer the highest volume of attacks. Because routers are the gateway for smart devices to connect with the Internet, compromising a router means gaining access to every unsecure device that uses it. The recommended course of action would be to purchase devices that are known to have security built in and that sit on frameworks that are also secure and can handle encryption, authentication, firewalls, etc.

"Low hanging fruit" may also be mined by looking for vendors that have frameworks which use certificate pinning – allowing only HTTPS-related certificates it expects to see before connecting to anything in the framework. The IP address is the most important element of the device. This unique identifier allows a company to identify the device sending or receiving the information. Communications or Internet connectivity allows the device to communicate with each other. As an increasing number of devices communicate with each other on an IIoT network, they will need to be authenticated either by digital certificates, biometrics, two-factor authentication or M2M authentication.

Conclusion

In conclusion, Accenture estimates that IIoT might add $14.2 trillion to the world's economy by 2030. 98.17% of all US companies have less 100 employees. That represents a lot of companies seeking to generate the significant economic gains that the adoption of IIoT promises, through productivity improvements and operational cost reductions. It also represents a lot of opportunities for catastrophic cyberattacks – 62% of all cyberattacks hit SMBs. The worst case scenarios could be averted if SMB organizations where to simply implement fairly rigorous and consistent cybersecurity frameworks.

There are many low cost/high impact solutions available today. SMBs just need to partner with integrators that can design for them an IIoT "minimum viable product" (MVP) that will be capable of reducing their cyber risk.

1. SMB Owners Lax About IoT Security Risk: https://www.pymnts.com/news/security-and-risk/2018/nationwide-study-smb-owners-iot-cybersecurity-risk/
2. Ibid. SMB Owners Lax About IoT Security Risk.
3. Stack, Tim. "Internet of Things (IoT) Data Continues to Explode Exponentially" Cisco, February 5, 2018, blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how
4. "IoT devices being increasingly used for DDoS attacks; Malware is infesting a growing number of IoT devices, but their owners may be completely unaware of it". Symantec Security Response, September 22, 2016, symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks
5. Gregory Garrett, December 13, 2018, Cyberattacks Skyrocketed in 2018. Are You Ready for 2019?, Industry Week, https://www.industryweek.com/technology-and-iiot/cyberattacks-skyrocketed-2018-are-you-ready-2019
6. Symantec, 2014 Internet Security Threat Report, 6 (Apr. 2014), Symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
7. Ibid. Symantec, 2014 Internet Security Threat Report,
8. Your SMB is at risk: 10 cyber-security trends to watch out for in 2018, Netcetera, https://www.netcetera.ca/cyber-security-trends/
9. National Institute of Standard and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, https://doi.org/10.6028/NIST.CSWP.04162018