sparton

Cybersecurity and Design

Managing New Risks and Requirements

Conquering Complexity®

Manufacturing has long been perceived as having lower cybersecurity risk than retail or financial industries. But the cybercrime landscape is always changing. Hackers are broadening their scope to include traditionally low-risk industries, and they're targeting areas of weakness along the chain that links designers, suppliers, and manufacturers. More than ever, it's essential that design engineers in medical, military and other industries understand the risks and take steps to avoid breaches that expose intellectual property and impact revenue as well as reputation.

The new cybercrime landscape

Malware, phishing, ransomware, social engineering, SQL injections—hackers are using old tactics in sophisticated new ways to target industries that may be lagging behind in the war against cybercrime. For example, the sensitive nature of healthcare data—and the increasing connectivity of "smart" medical devices—makes device makers and their partners more attractive to hackers. Expectations and awareness are also changing as new government guidelines and programs get underway.

sparton

A focus on supply, manufacturing

Retail and financial industries are often perceived as higher risk than manufacturing because of their large, decentralized structures and high volumes of sensitive consumer information. However, hackers have discovered that points along the design, supply and manufacturing chain offer rich, easily accessible stores of data. It turns out that even

40 percent of data-security breaches arise at points where companies, suppliers and other partners interact

in retail breaches a supplier is often involved. For example, the recent attack on Target stores that compromised the data of 70 million customers occurred through a refrigerator supplier's access. Research shows that about 40 percent of data-security breaches arise at points where companies, suppliers and other partners interact. According to one industry insider, most cybercrime today occurs outside of finance and retail: "financial services gets more press, but industrial networks get more attacks."[1]

New guidelines increase expectations, awareness

An important element in the cybercrime landscape is the new cybersecurity framework developed under executive order by the National Institute of Standards and Technology (NIST), now part of the U.S. Department of Commerce. The NIST framework is aimed at protecting U.S. infrastructure, which encompasses dozens of industries including defense, healthcare, IT, critical manufacturing, chemicals, energy, emergency services and more. The U.S. government is also putting special attention on medical devices. The FDA recently issued draft guidance regarding postmarket management of security risks that focus on adverse or fatal health consequences. It's clear that clients will expect products to be designed and produced in a way that aligns with these guidelines. What's more, the guidelines may evolve into federal regulations. Companies that plan now to adopt them will be ahead of the game.

The Obama Administration's Cybersecurity National Action Plan (CNAP) is implementing several initiatives that may further raise awareness among clients and end users. "The focus of CNAP is to improve awareness in both the public and private sectors," says Jim Janicki, Business Unit Director of software development at Sparton. "It's intended to accelerate awareness, engage vendors and assist in communicating those vulnerabilities to various stakeholders."

Re-emerging threats

Think email is a cybercrime of the past? Malicious attachments started reappearing in 2014 and dramatically increased in 2015. The difference today is that hackers aren't blanketing large groups with email — they're using sophisticated methods to target those with access to IP, financials and other valuable data. Often these emails have highly specific requests and are carefully masked as communications from the CEO, CFO, comptroller or an upper-level manager. Hackers study social media to extract names and details and to learn what type of request is likely to be answered. Emails are timed for moments when the team is in full swing — the highest points of successful entry occur on Tuesdays at around 10:00 am.[2]

Cybercrime stemming from inside the organization is also on the rise. A survey by the nonprofit Information Systems Audit and Control Association (ISACA) found that nearly 40 percent of incidents in 2014 arose from nonmalicious insiders, and 28 percent were caused by those intentionally trying to steal from or damage their organization.[3]

1 Spiegel, Rob. "Manufacturing becomes the biggest cyber attack target." *DesignNews*. Web. January 10, 2016. www.designnews.com.

2 Miller, Jen A. "Four new cybercrime trends that threaten your business." *CIO Online*. Web. September 7, 2015. www.cio.com.

3 State of cybersecurity: implications for 2015. *ISACA and RSA Conference Survey*. Web. 2015. www.isaca.org.

sparton

Where are the primary vulnerabilities?

It's important to keep in mind that the new government guidelines do have limitations and don't always address vulnerabilities further up the chain. For example, security experts warn that the FDA medical device draft guidance on postmarket risk management "cannot substitute for a thorough evaluation of vulnerabilities before a device reaches the market."[4] This evaluation may include modifying the design to mitigate those risks—additional hardware, a change in software, or any number of enhancements or changes. From a software perspective, the communication part of the package is likely the most vulnerable and worthy of risk assessment.

"The communication module is where a lot of the vulnerabilities come into play," says Janicki. "Consider what will be received by the module, handling something unexpected, sending something that isn't received or is garbled in some way. Isolating the communication module as much as possible allows you to keep the major product functions performing even if there's a hiccup with the communication."

And what about the period between design and outside manufacturing? For design engineers concerned about cybersecurity, communication with suppliers and the transfer of files to an outsourcing partner deserves special attention.

"One of the most vulnerable or unsecure points in the process is how information gets here," says Chris Ratliff, Vice President of Information Technology at Sparton "We often see files arriving over email, or sensitive business information shared in files and on drives that aren't password protected. As information travels, there's not only the intellectual property that's at risk, but pricing and cost information—details that would enable competitors to effectively undercut the offering. Any information about suppliers and financials is also highly valuable to a hacker."

According to Ratliff, the security of file and information transfers can be dramatically improved though encryption or authenticated FTP sites—but the team has to be willing to take a few extra minutes to ensure security.

"One of the most vulnerable or unsecure points in the process is how information gets here ... there's not only the intellectual property that's at risk, but pricing and cost information ... highly valuable to a hacker."

Chris Ratliff
Vice President of Information Technology at Sparton

4 Hartford, Jamie. "Five takeaways from FDA's draft guidance on postmarket management of cybersecurity risks in medical devices." *MDDI*. Web. March 21, 2016. www.mddionline.com.

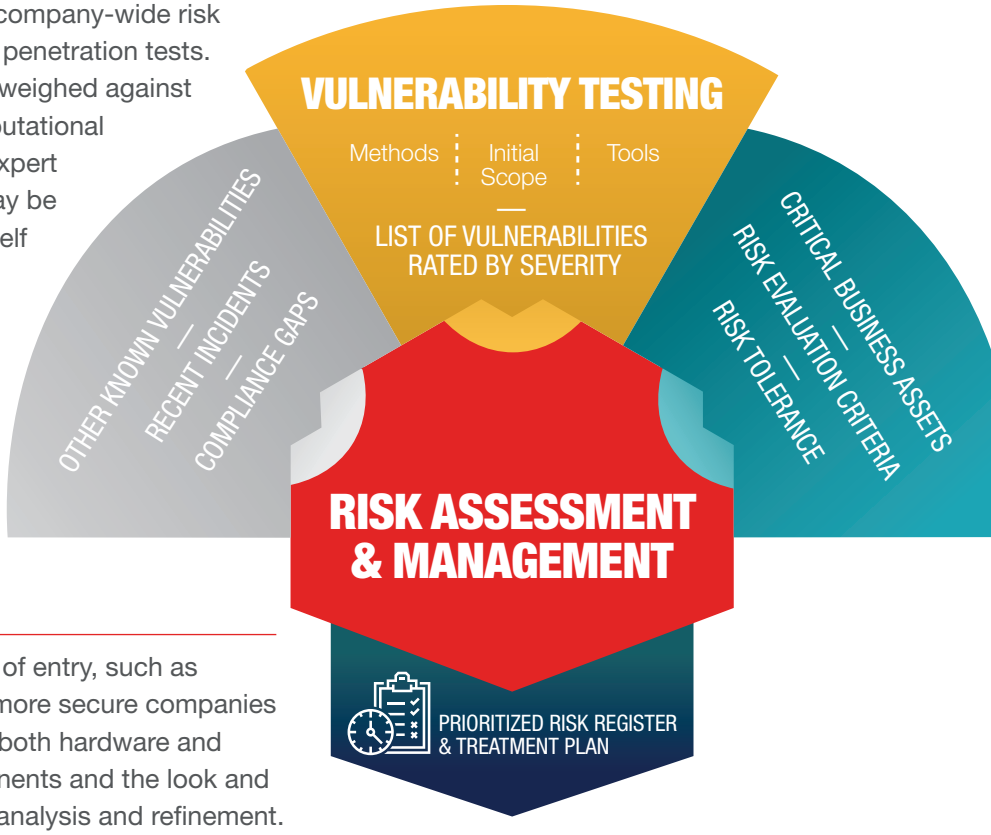
sparton

Key steps in prevention

Beyond taking precautions with transferring design files, design engineers and their partners have several opportunities for dramatically enhancing cybersecurity and improving business operations.

1 CONDUCT A RISK ASSESSMENT

Risk management experts recommend a company-wide risk assessment along with individual, one-off penetration tests. The risk of each vulnerability can then be weighed against the cost of a fix and the operational or reputational impact of each potential breach; as one expert noted, "elimination of all negative risks may be neither possible nor desirable and may itself jeopardize performance of the device."[5] Such a "risk register" is ideally presented to board-level leadership to ensure clear understanding of current levels of risk and whether or where investments should be made.



2 BUILD A "MOAT"

Cybersecurity used to focus on one point of entry, such as installing an Internet firewall. But today's more secure companies design products with layers of security in both hardware and software, making modifications to components and the look and feel of products in a process of continual analysis and refinement.

"It requires thinking in reverse and asking up front, 'What if we get hacked?' 'What's our risk?'" says Ratliff. "Keep the castle analogy in mind. Cybersecurity is all about layers, and it's no different from security in medieval days. Castles were built on hills—that's one layer. They had big brick walls—that's another layer. There was a drawbridge, a moat and archers shooting arrows—more layers. One or two layers might not stop someone, but together they can increase security and make the hacker feel it's not worth the effort. Some layers are inexpensive, and others are costly. But given the potential losses, it's worth putting more effort into risk analysis of the design and the design process.

5 Why you should adopt the NIST cybersecurity framework. *PricewaterhouseCooper, LLP*. Web. May, 2014. www.pwc.com.

sparton

3 ENGAGE PARTNERS AND SUPPLIERS

Design engineers and others involved in creating or modifying products should be paying more attention to the security of their suppliers and partners. A few simple direct questions or a checklist will make it clear whether there's potential for risk.

"Your suppliers and partners are an extension of your product," says Ratliff. "Ask them, 'what type of policies do you have in place?' What certifications do you have or are you working toward?' 'What off-the-shelf security products do you use?' How do you test products?' But be aware that the lower you go in the supply chain, the less you'll hear. Smaller companies or those offering lower pricing have fewer investments in security protocols. With even a brief conversation, it should be easy to gauge your level of risk."

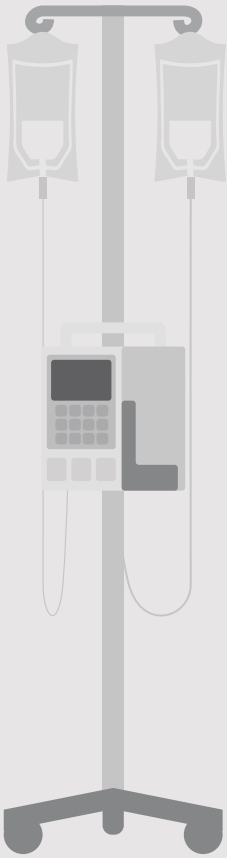
A robust security policy provides a strong selling point in a competitive market with customers who understand what's at stake.

4 ADOPT AND MARKET

Adopting the voluntary FDA and NIST guidelines can provide a solid starting point for strengthening cybersecurity in product design and production. In addition to protecting IP, data, revenue, and reputation, other benefits may stem from more rigorous cybersecurity practices. For example, a robust security policy provides a strong selling point in a competitive market with customers who understand what's at stake. Designers can play a key role in the integrity and approach of these internal security protocols.

Hacktivists put spotlight on medical devices

Several so-called "hacktivists" — those with good intentions — discovered that a widely sold hospital infusion pump was vulnerable to attack. The device delivered dosages that could be altered externally by someone other than a doctor or nurse. In one case, the Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (ICS-CERT) was contacted. The incident resulted in the FDA's first warning against using a device because of cybersecurity weaknesses. The manufacturer called on Sparton to step in, and we worked with the design engineers to close the cybersecurity gaps in this product space.



Our deep experience as a contract design and manufacturer for an array of complex products gives us unique insight and expertise with security issues not always available to internal staff or other manufacturers.

sparton

Conclusion

There's one final benefit to prioritizing cybersecurity within the organization: ***it nurtures collaboration.*** This, in turn, strengthens awareness and compliance. According to one report, 82 percent of companies with high performing security practices also have a high degree of internal communication and collaboration.[6] However, because sharing information presents its own risks, it's prudent to begin any initiatives with security experts and partners who have a high degree of knowledge about cybersecurity in the design and manufacture of critical products.

6 Hartford, Jamie. "Five takeaways from FDA's draft guidance on postmarket management of cybersecurity risks in medical devices." *MDDI*. Web. March 21, 2016. www.mddionline.com.

About Sparton

Sparton offers design and manufacturing expertise to leading companies in the medical and biotechnology, military, aerospace and industrial and commercial industries. Sparton incorporates advanced cybersecurity protocols and rigorous risk analysis and mitigation into its process. We leverage the knowledge, experience and resources of 13 U.S. sites to improve cybersecurity for critical manufacturing needs. For more information, visit www.sparton.com.

SPARTON CORPORATION

425 N. Martingale Road, Suite 1000
Schaumburg, Illinois 60173
800.772.7866
www.sparton.com