Shannon & Associates LLP
Certified Public Accountants
Management Consultants

Manufacturing & Distribution Advisor

COMMITTED TO YOUR SUCCESS

Fall 2014

ARE YOUR INFORMATION SYSTEMS SECURE?

Warning: Your computer systems have been hacked. It's the news no executive team wants to hear, but it's increasingly commonplace in today's interconnected world.

In July 2013, Apple Inc. experienced a high-profile cyber attack on its developer website. In the aftermath, the smartphone, tablet, and computer manufacturer publicly admitted that the culprits made off with an unknown number of mailing lists, e-mail addresses and possibly other sensitive personal data. Here are some ways manufacturers and distributors can prevent a similar data breach from occurring at their facilities.

Know your risks

Cyber attacks are estimated to cost U.S. businesses as much as $250 billion per year, according to computer security firm Symantec. And it's not only large multinational businesses that are targeted these days.

According to a 2013 study by the Ponemon Institute, a data protection and information security research firm, 29% of U.S. small businesses experienced a computer security breach during the previous year. Of those attacked, nearly three-quarters of the victims were unable to fully restore their systems after the attack.

The survey also reports that the consequences of those attacks included potential damage to their reputations (59%); theft of business information (49%); the loss of angry or worried customers (48%); and network and data center downtime (48%).

Manufacturing and distribution executives sometimes can be caught unaware of the prevalence of computer security breaches; mistakenly presuming that cyber attacks and network disruptions happen primarily in other sectors, such as health care and retail.

But manufacturers and distributors rely heavily on electronic data systems; for example, to transfer freight manifests, track inventory with RFID tags and dispatch load routes. So, they can't afford to take a reactive approach to information technology (IT) security.

Prepare your defenses

Prevention is essential when it comes to making sure malicious hackers don't vandalize your information systems or make off with your plant's valuable trade secrets, customer lists or financial information. Here are some ways you can minimize the chances of becoming the victim of a cyber attack:

Inventory your data. Catalog where you store customer lists, financial information and inventory information, so you can assess its vulnerability. It may not always be on site. For example, some information may be stored on personal computers in the possession of current and former employees.

Assess risk. In-house or outside IT professionals can help analyze weak spots. They can determine whether you possess the most effective, up-to-date software available to protect against dangerous virtual predators like worms, malware, trojans and viruses. It's also a good idea to change passwords on a monthly basis and encrypt sensitive data transmitted electronically.

Communicate with vendors. Data security is a collaborative effort among all of a company's partners. For example, if you grant a third-party shipping company access to proprietary supply chain data (such as your customer's demand and inventory levels) that information could be stolen if a hacker breaches the shipping company's computer systems.

Limit data sharing to only those supply chain partners that absolutely need it. And ask your partners about their IT security programs. Request partners with weak IT controls to beef up their efforts.

Protect your business

Unfortunately, some businesses don't know that their systems, intellectual property and important business records are vulnerable to cyber attacks until it's too late. Check with your advisor today to ensure that your financial information is secure.

IN THIS ISSUE

THE TRANSFORMATION OF MANUFACTURING - AGAIN

by Bill Virgin

Manufacturing as we think of it today doesn't look much like it did 25, 50 or 100 years ago, in terms of what manufacturers make, how they make it and what they make it with.

And why should it? Few other business sectors operate as they did even (in some cases) a decade ago. The ubiquity of smart phones, combining camera, computer and telecommunications device into one handheld unit, disguises the fact that such devices as mass-market consumer products are less than a decade old.

Manufacturing has gone through huge transformations in its history, from sources of power (water to steam to electricity) to the level of sophistication of products, the reach of supply and distribution chains (from local to global) and methods of production (interchangeable standardized parts, moving assembly lines, robotics).

Manufacturing often has to shake off the perception that it doesn't change at all, never mind at a slower pace than other sectors. No doubt manufacturing executives find it tiresome to have to explain one more time that their operations do not resemble a steel mill circa 1954 (even steel mills, those that are left, don't much resemble their ancestors).

But it is changing, all the time. There are at the moment multiple transformations going on in manufacturing, some mature to the point of widespread acceptance, others in their earliest days but with great promise.

Two prime examples of the former are robotics and composites. Industrial robots have been around for decades; even the most casual observer of manufacturing is familiar with car-company television commercials depicting robotic painters and robotic arms swinging components into place.

Robotics represents a transformative technology, but it's not been a fast or smooth revolution. Much of the early hype over industrial robots dissipated because of the cost of the systems and production snarls and snafus (stories still linger about early-generation robots painting each other because of programming glitches).

But manufacturers didn't give up on the idea of robotic systems. Instead they improved and refined the robots and found new applications for them. Boeing recently completed testing of a new method of assembling 777 fuselages in which robots install 60,000 fasteners currently placed by hand. The company had been testing the assembly method at a facility in Anacortes, and intends to install it in a new facility in which the 777X will be built. Boeing believes the new system will reduce build times and worker injuries and increase quality.

Robots are also being employed for inventory management, for delivering parts and work-in-process to production stations and for moving pieces between machines. As with most technologies (think of smart phones) the applications and capabilities are increasing while the costs are coming down. The cost of a robotic vacuum cleaner has been driven down to the point that households can afford them. The same phenomenon applies to more sophisticated industrial systems.

If robots are a standard feature in manufacturing operations, composites are rapidly becoming a standard material with which manufacturers work. At the Society for Advanced Materials and Process Engineering's annual convention, held in June in Seattle, the full range of composite-based products made by Washington companies was on display: Sporting goods, including fly-fishing rods. Guitars. A radar dish. Car parts (even though the state is thousands of miles from the nearest auto assembly plant). Snowboards. A prosthetic foot. And that doesn't include the stuff too big to fit in an exhibition hall, like airplanes and yachts.

The use of composite materials will expand, but already manufacturers are toying with the next generation of materials, including nanolaminates, as well as a film or coating that can be applied to glass and transform solar energy into electricity.

The "Next Big Thing" in manufacturing, one just about everyone has seen a demonstration of, is 3-D printing in which resins or metal can be deposited, somewhat like a spider spinning a web, to make an object.

Artists were the early experimenters with 3-D printing. The health-care

continued on page 3

THE TRANSFORMATION OF MANUFACTURING - AGAIN

continued from page 2

industry is finding the customizable features of 3-D printing (also referred to as additive manufacturing) attractive for making artificial joints and dental implants designed to fit individual patients.

Manufacturers were initially interested in 3-D printing as a way of cutting the modeling and prototyping time needed in developing new parts and products. It's one thing to design a part on a computer, as most companies do. It's a huge step forward to take that digital file, feed it into a 3-D printer and have it produce a physical object in a matter of hours, reducing the time it takes to make changes and produce another prototype or model.

Once again, a technology transforms itself as it transforms the businesses employing it. Three-dimensional printers are getting cheaper and faster, to the point they're not an exotic technology beyond the reach of small and medium-sized companies.

That progression has some in manufacturing wondering if 3-D printers might be used for actual finished-item production. The cost and time make that unlikely for all but the most customized parts where expense is not an issue. But that's today. Who wants to bet that 3-D printing technology will be where it is now in as little as five years?

What manufacturers make with these technologies is changing too, at too fast a pace to be called evolutionary. At least half a dozen Washington manufacturers are now working on products incorporating LED lighting, a replacement for incandescents and fluorescents that is finding its way into outdoor, residential and commercial lighting.

Change, disruption, upheaval, all can be unsettling at times. For manufacturing, these transformative technologies are positive and necessary. You want to see them. Without them, what you're left with is a sector that is stagnant, declining, uncompetitive, irrelevant and – last and least – extinct.

Bill Virgin is a veteran business journalist and the founder of the newsletters Washington Manufacturing Alert and Pacific Northwest Rail News. He is also a columnist for The News Tribune, Seattle Business Magazine, and the energy newsletter Clearing Up. He and his wife own Page 2 Books, a retail store in Burien.

CAN YOU AFFORD THE RISK?

by Jessica Kinney, CPA, CFE, Manager

As an owner or executive, the greatest assets you protect are the value, reputation and employees of your company. Setting the right tone at the top is vital for cultivating a culture that displays a desire for avoiding costly mistakes, an appreciation for strong controls, and a zero-tolerance attitude towards fraud.

Protecting value

The positive reputation of your business drives value. An ethical tone at the top protects your company's goodwill. Employees who are aware of management's adherent interest in securing its assets, by closely monitoring its controls are less likely to act unethically. Communicating an atmosphere of strong oversight and zero-tolerance is vital to reducing exposure to damaging behavior.

Protecting the bottom line

External pressures may distract you from internal opportunities and risks. Opportunities to reduce costs may be missed, poorly supervised or fatigued staff may make unintentional but costly mistakes, available discounts may be ignored and poor internal controls may allow employee fraud.

Can you afford these risks?

Taking action

Surprise Audits. The element of surprise is very powerful in setting a zero-tolerance tone. On a periodic basis it is important to test technical and procedural controls and operational processes. Employees should not be notified in advance of the area being tested. Instilling this process encourages employees to be attentive to identifying areas that could be susceptible or are already at risk for lost earnings. Additionally, surprise audits can be a powerful tool for identifying costly mistakes. "Victims who undergo surprise audits average $93k in losses. Those who don't average $164k"*

Red Flag Audits. Your accounting data tells a story, understanding it is half the battle. Sometimes by running some quick queries using proven statistical and logical methods, we can identify anomalies in your everyday transactions that suggest potential fraud or abuse.

Fraud Hotline/Webline. Implementing safe and private avenues for employees to communicate suspicious behavior encourages employees to report red flags - without fear of repercussions. "Victims who have a hotline average a loss of $100k. Those without average $168k" *

IT Audits. As technology becomes easier and more accessible, so does fraud. Understanding the weaknesses inherent in the systems you use for operations and communication. Being proactive with your technology security and its processes will provide an air of accountability and continuous development with your internal service providers.

Improving Controls. Looking at implementing an improvement plan on how to tighten or enhance your controls and operations.

Strong Policies. Employees will receive tools for taking safe and appropriate action when suspicions develop. Having documented policies in place will protect your organization and clearly communicate to your employees, investors and shareholders that your organization is proactively committed to operational excellence.

Employee Surveys. Knowing in advance if your employees have concerns about fraud or ethics can help you resolve problems before they become lawsuits or significant losses.

Employee Training. A key step to communicating high expectations is educating your employees on where to look for fraud and what to look for. Having yearly training sets the tone that your organization is not complacent when protecting its assets. "42% of frauds are found by someone speaking up" *

Stop worrying about what you can't control and start focusing on what you can control. Protect your value, improve your bottom line. Give us a call to discuss how we may be able to assist you.

*Association of Certified Fraud Examiners - 2014 Report to the Nation.

SHANNON & ASSOCIATES, LLP
Certified Public Accountants & Management Consultants
1851 Central Place South, Suite 225, Kent, WA 98030 | 253-852-8500
info@Shannon-CPAs.com | www.Shannon-CPAs.com