BANK OF THE WEST

BNP PARIBAS GROUP

Fortifying Your Business:
Fraud and Security Measures for U.S. Manufacturers

By **David Pollino, Fraud Prevention Officer**

August 2015

It won't happen to me.

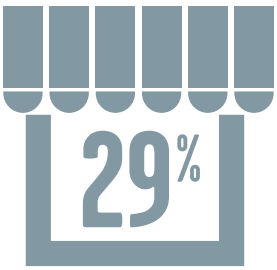
In today's interconnected world where businesses increasingly rely on data and networks, sophisticated cyber-crime groups can inflict as much damage as natural disasters.

Conversations with our small- and medium-size manufacturing clients, our own research, and recent reports paint a picture of rising security threats. Although they are susceptible to three security threats in particular, smaller manufacturers often feel that they don't face the same threats bigger companies do. "We're not Target," they say. Or, as one manufacturer put it, "We're such a niche business, I think we're under the radar."

We've long suspected that many small business owners aren't taking the necessary precautions; as early as 2013, we confirmed that security and fraud threats tend to be a low priority among small business owners. Our report, "Fighting Fraud: Small Business Owner Attitudes About Fraud Prevention and Security,"[1] revealed that awareness and investments in security spike after a business suffers an attack. Today, small- to medium-size manufacturers face an even greater risk and cannot afford to wait until after an attack to protect their businesses.

"A lot of companies think it's not going to happen to them, and they don't put a huge emphasis on Internet security. Everything is a matter of priorities in a small company, and that's not at the top of their list," said one Midwestern manufacturer who struggled a few years ago with an accounting system corrupted by a virus.

The data show that small businesses are actually victimized more than any other business size category, according to the Association of Certified Fraud Examiners' 2014 Report to the Nations on Occupational Fraud and Abuse.[2] Nearly 29 percent of cases reported came from small businesses.



Small businesses are disproportionately victimized by fraud. Nearly 29 percent of fraud cases reported came from small businesses

Source: Association of Certified Fraud Examiners

While small businesses are certainly susceptible to a wide array of threats, there are three that stand out as particularly important for manufacturers: **masquerading**, **intellectual property theft**, and **cybersecurity breaches**. The good news is that there are relatively low-cost preventive measures to help bar the door against each of these risks.

MASQUERADING

For the third consecutive year, three in five companies were targets of payments fraud, according to the Association for Financial Professionals' 2015 Payments Fraud and Control Survey.[3] As small- and medium-size manufacturers expand[4] domestically and internationally — broadening their networks of vendors, business connections, and customers — the risk of payments fraud rises.

In 2015, for the third consecutive year, three in five companies were targets of payments fraud.

Source: Association for Financial Professionals

Masquerading[5] is a payments scheme in which a fraudster impersonates a company executive or outside vendor and requests a wire transfer through a phone call or email to a company controller, or someone else with authority to wire funds. The controller will usually tell the business's bank to wire the funds because the email or phone call seems legitimate.

Even a precautionary call from a bank's fraud-prevention department to double-check a wire transfer may not stop a masquerading attack. Typically, the person at the business ordering the transaction insists the wire transfer request is legitimate and verbally authorizes the bank to proceed. Since these fraudulent wire transfers frequently go overseas, it can be very difficult to recoup the funds.

"The mistake we all make is we think it is not going to happen," said the CFO of a West Coast company whose products are contract-manufactured in Asia. After receiving an email request from a fraudster masquerading as one of its vendors, the business wired tens of thousands of dollars to an overseas bank. "If you had asked me before it happened whether I expected someone to use email to act like somebody else to take money from me, I would have said, 'Of course not.' I didn't think of that as a risk. That someone could masquerade as my supplier to try to get money? I never thought that was a reality."

Four simple steps to help manufacturers thwart masquerading attempts:

1. **Develop an approval process for large transactions.** Require approval from two or more executives for large wire transfers to protect against internal and external fraud.

2. **Use a purchase order model for wire transfers.** Many companies require a purchase order number to spend money. Apply this model to match all wire transfers to a purchase order reference number, which provides another layer of control by requiring an approval for wire transfers and a verification of that approval.

3. **Confirm and reconfirm.** Use multiple means of communication to verify wire transfers are legitimate. If the initial request comes in email, then call the person to get a verbal confirmation and vice versa.

4. **Stay in touch with your bank.** If a transaction seems suspicious at any point in the process — even after a wire has been sent — contact your financial institution immediately.

INTELLECTUAL PROPERTY

Intellectual property is vital to manufacturers. Product blueprints and trade secrets are essentially the "keys to the kingdom." With them, practically anyone can replicate your product. Manufacturers ranked theft of trade secrets as their fifth biggest concern and intellectual property theft as seventh, according to the 2014 Top Security Threats and Management Issues Facing Corporate America[6] survey from Securitas. In contrast, other industries ranked these concerns 17th and 19th, respectively.

"The highest probability of theft is going to come from employees, because the people closest to you are the ones who are going to have access. That is the biggest risk: employees who then become your competitors," said an executive at a California manufacturer, who described protection of several high-value products under a pending patent as "the No. 1 concern for our company."

Protecting intellectual property requires screening employees and vendors as well as securing networks, computer devices, and equipment against intrusion from malware[7] and spyware, malicious software that can disrupt devices and networks or capture confidential data and send it to hackers.

Manufacturers See Intellectual Property as Top Threat

Manufacturers Ranked	All Industries Ranked	Security Threat
1	1	Cybersecurity
2	3	Workplace Violence
3	2	Business Continuity Planning
4	4	Employee Selection
5	17	Theft of Trade Secrets
6	20	Global Supply-Chain Security
7	19	Intellectual Property/ Product Counterfeiting

Source: Securitas

How to get started protecting intellectual property:

1 Definitions.
Define what constitutes the business's intellectual property. *Is it a product, a process, R&D, source code, or a logo design?*

2 Storage.
Identify all the places this intellectual property is stored or located. *Is information related to the company's trade secrets in printed blueprints, on a server, locked in a vault, programmed into equipment on the manufacturing floor, or in an email?*

3 People.
Maintain an up-to-date list of who knows about company trade secrets, both inside and outside the company. *Are they under non-disclosure agreements and other terms that protect the business?*

4 Access.
Give employees, vendors, and others the least amount of access possible to do their jobs. The more people who have access, the greater the risk.

CYBERSECURITY

As manufacturing has become increasingly automated, digital assets such as websites and email have become vulnerable to a range of cyber-attacks—from criminals determined to plant spyware to track and steal secrets to denial-of-service attacks that overwhelm company websites.

"We have had our website hacked on a number of occasions, and it is very expensive," an executive at a California manufacturing business said. "Our vulnerability isn't as great as a Target or a Home Depot where they're storing customer data, but we're still subject to the same threats."

Six simple steps to help protect against email and website attacks:

1. **Install anti-virus protection** on every computer and device on the company's network.
2. **Educate employees** to recognize, avoid, and report suspicious emails containing attachments or hyperlinks, the telltale signs of phishing[8], in which hackers use electronic communications to steal sensitive information.
3. **Be discerning with privilege.** Employees and outside vendors using a company's network should have access to only those applications that their jobs require.
4. **Enforce two-factor authentication**[9] for administrative access to the company's critical servers. Verifying a user's identity through separate channels — text or email, for example — helps prevent anyone from having access to a device without first confirming his or her identity through an alternate means of communication.
5. **Ensure software and operating systems are current** and that updates are installed quickly.
6. **Maintain a separate administrator account** with a unique password so that if an IT administrator's primary email or passwords are compromised, hackers will still not have administrative rights to gain control of servers and networks.

Secure Your Business

The day-to-day pressures on small- and medium-size manufacturers make it tempting to put security aside. But the potential costs grow with each passing day as more sophisticated threats emerge.

"Data has become so crucial," said the Midwestern manufacturer whose accounting system was attacked by a virus. "If you take a step back and look at what would happen if you lose it, then it becomes clear that security is an important factor we need to address."

As another executive put it, "With today's technology, some of these crimes are like natural disasters. If your system shuts down and you can't get that data, you could be down for weeks, months, maybe forever."

The stakes are high, but manufacturers can help themselves mitigate common threats like masquerading, intellectual property theft, and cyber espionage. Simple measures today can go a long way toward fortifying your business for the future.

ENDNOTES

1. Bank of the West, *Fighting Fraud: Small Business Owner Attitudes About Fraud Prevention and Security* (Bank of the West, 2013), web, http://GoWe.st/sklj.

2. Association of Certified Fraud Examiners, *Report to the Nations on Global Fraud and Abuse* (ACFE, 2014), PDF file, http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

3. Association for Financial Professionals, *AFP Survey: Financial Professionals Confident That EMV Cards Will Help Mitigate Credit/Debit Card Fraud* (AFP, 2015), web, http://www.afponline.org/PressReleases.aspx?id-8589936473.

4. Scott Anderson, *Made Here: The Business Outlook for U.S. Manufacturing* (Bank of the West, 2015), PDF file, http://GoWe.st/mfg1.

5. David Pollino, *60 Security Download: Masquerading* (Bank of the West, December 19, 2014), YouTube video, 1.06, http://GoWe.st/Masquerading.

6. Securitas Security Services USA, *Top Security Threats and Management Issues Facing Corporate America* (Securitas Security Services USA, 2015), PDF file, http://www.securitas.com/Global/United%20States/Knowledge%20Center/2015%20Top%20Security%20Threats%203-27-15%20REV%20C.pdf .

7. David Pollino, *.60 Security Download: Malware* (Bank of the West, December 19, 2014), YouTube video, 1.02, 2014, http://GoWe.st/Malware.

8. David Pollino, *.60 Security Download: Phishing* (Bank of the West, December 19, 2014), YouTube video, 1.07, http://GoWe.st/Phishing.

9. David Pollino, *.60 Security Download: Two-Factor Authentication* (Bank of the West, December 19, 2015), YouTube video, 1.12, http://GoWe.st/2FactorAuthentication.