Small Businesses, Big Threats

The growth company CFO's guide to protecting your data.
<table>
<thead>
<tr>
<th>Chapter Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword: Is Information Technology Insecure?</td>
<td>5</td>
</tr>
<tr>
<td>Risky Business: SMB Vulnerability</td>
<td>6</td>
</tr>
<tr>
<td>Don’t be Fooled: Why SMBs are Easy Targets</td>
<td>7</td>
</tr>
<tr>
<td>Wiping the Slate Clean: Digital Copier Danger</td>
<td>9</td>
</tr>
<tr>
<td>Murky Skies: Cloud Security Risk</td>
<td>11</td>
</tr>
<tr>
<td>Data Breach: The Reality of Cyber Attacks</td>
<td>13</td>
</tr>
<tr>
<td>In the Dark: Denial of Service</td>
<td>14</td>
</tr>
<tr>
<td>Clever Criminals: The Evolution of Fraud</td>
<td>17</td>
</tr>
<tr>
<td>How To Be Prepared: Small Business Protection</td>
<td>19</td>
</tr>
<tr>
<td>Playing It Safe: Cyber-liability Insurance</td>
<td>20</td>
</tr>
<tr>
<td>For Better or for Worse: Secure Collaboration</td>
<td>22</td>
</tr>
<tr>
<td>Lock your Doors: Preventing a Breach</td>
<td>24</td>
</tr>
<tr>
<td>Conclusion: Successful SMB Security</td>
<td>26</td>
</tr>
</tbody>
</table>
When the website of the Central Intelligence Agency and the phone systems at the Federal Bureau of Investigation can be hacked, as they both were earlier this year, it gets one wondering just how secure all that corporate data is on our smartphones, tablets, laptops and even old-timey on-premises desktops. For small and medium sized businesses, such worries are multiplying—for good reason, too.

Hackers increasingly target midsized and smaller companies, looking to steal their intellectual property, competitive data and the personally identifiable information of employees and customers. This treasure trove of data is a kind of currency that is then sold to organized criminal elements for credit card fraud and other illicit moneymaking schemes. SMBs are in the crosshairs because they’re perceived as easy prey, with inferior security protocols, processes and systems when compared to their larger counterparts.

This perceived vulnerability was exploited before social media, mobility, Big Data and the Cloud converged to create entirely new ways of doing business, and is even more so in its aftermath. Mobile business apps now populate the miniature landscapes of smartphones and tablets, predicated on making every executive from the CFO down to the rank and file more personally productive. These apps typically are integrated with back-end ERP, CRM, HRMS and supply chain systems to grease the wheels of operations. The net effect is a lot of sensitive data roaming out there in the Cloud.

And it’s all roaming at the same time that hackers continue to become more sophisticated in their methods. What can small and medium size businesses do? That’s the subject of this e-book, which illustrates the security threats posed by hackers, the information they’re looking to get their dirty hands on, and posits ways to defend this data and attack back.

The bottom line for readers is that the seriousness of these security risks cannot be overestimated—once a data breach is made public (companies are compelled by law to report the incidents to federal and most state authorities), the reputational exposures loom large. Big companies may be able to withstand the financial effects of reproachful customers, but not all small and midsized organizations can endure this burden.

Certainly, there is a dire need for finance to take a more active role in identifying the sources of data security risks and positing ways to mitigate, manage and transfer the related financial costs. Time is of the essence—hackers pride themselves on being one step ahead.

--Russ Banham
“A recent Symantec survey of more than 2,000 small and midsize enterprises found that 73% had been victimized by cyber attacks, and the cost cannot be measured by dollars alone. ‘There’s always the risk of customers no longer conducting business with you. Once your reputation is tarnished, shutting down becomes a very real possibility.’”
DON’T BE FooLED: WHy SMBS Are EASY TARGETs

YesterdAY’S hackers, whose exploits were often designed to earn bragging rights within the hacker community, have given way to far more sophisticated cyber criminals in pursuit of cold, hard cash. Some penetrate databases to steal the personally identifiable information (PID) of employees and customers. Others steal intellectual property and business data. Some use it, while others sell it to other criminals.

Which companies are hackers targeting? “The main focus of hackers seeking PID is midsize companies,” says Paul Viollis, CEO of Risk Control Strategies (RCS), a security and investigative firm. Why? “They’re perceived as the path of least resistance.”

Midsize organizations with up to 100 employees and $100 million a year in revenue “lack the security budgets of their big-business peers,” explains Tim Matthews, director of product marketing at Symantec, a leading security systems provider.

A recent Symantec survey of more than 2,000 small and midsize enterprises found that 73% had been victimized by cyber attacks, and the cost cannot be measured by dollars alone. “There’s always the risk of customers no longer conducting business with you,” Matthews says. “Once your reputation is tarnished, shutting down becomes a very real possibility.”

Social engineering—the art of tricking people—has caused more security breaches than all external attacks combined, according to 403 Web Security, a web-application development company.

Social engineering was behind a March 2011 data breach at security firm RSA. Employees received an e-mail and an attached spreadsheet with the subject line, “2011 Recruitment Plan.xls.” Once opened, the spreadsheet installed a backdoor in RSA’s system that compromised the code of RSA’s SecurID token. Estimates of what RSA’s parent, EMC, spent to clean up the fallout have run north of $66 million.

“We’ve estimated that a data breach costs companies an average of $214 per compromised record, and this excludes litigation and reputation-related issues that are difficult to measure,” says Larry Ponemon, founder of the Ponemon Institute, which focuses on data-protection practices.

Ponemon agrees that today midsize enterprises are in the crosshairs. “Why hack into a major retail bank that has topnotch security when you can hack into a much smaller enterprise that has access to the bank’s data?” Ponemon asks. “It’s easier to break into the side door than the front door.”
And those side doors aren’t locked at many midsize organizations. Of the 761 data breaches investigated in 2010 by the U.S. Secret Service and Verizon Communications’s forensics analysis unit, 63% occurred at companies with 100 or fewer employees.

Most of those breaches were not as sophisticated as the RSA hack. A recent Ponemon survey cites lost or stolen mobile devices as the greatest trending security risk. The risk doesn’t necessarily decline when the focus shifts. “Companies think because they outsource services or security they also outsource liability,” says Toby Merrill, vice president at insurer ACE Professional Risk. “They’re wrong.”

“You Will Be Sued”

Forty-six states have data-breach laws that require organizations to notify anyone whose personal data may have been compromised. Massachusetts’s is the toughest, stipulating penalties of up to $5,000 per violation. Multiply that by thousands of affected customers, and the potential cost to the enterprise is staggering. These laws make it clear that responsibility lies with the company that collected and stored the data. “That’s who will be sued,” Merrill says.

But many midsize businesses believe the cloud offers greater security. Boloco, a $20 million chain of 18 burrito restaurants stores customer information in the cloud via NetPOS, a point-of-sale systems provider. “No credit-card swipe lives in our system,” says Boloco CFO Patrick Renna. “Our philosophy is to leverage the security expertise of much larger companies that have resources we don’t.”

Boloco requires its various software-as-a-service providers to comply with the payment-card industry’s data-security standard and with the SAS 70 auditing standard, which permits an independent auditor to evaluate and issue an opinion on the provider’s security controls. Boloco also assesses its providers’ finances. That’s smart, says Tracey Vispoli, global cyber solutions manager for the Chubb Group of Insurance Cos. If you’re suing, you want your provider to be solvent.

Hack Counterattack

What else can midsize companies do? If they had the cash, they could hire a security guru, and implement encryption, firewalls, intrusion detection, and other security tools. But today, as RCS’s Viollis notes, “how many midsize enterprises have cash to spare?”

There are, however, measures that won’t break the bank, notes Alan Wlasuk, CEO of 403 Web Security. He suggests starting with a relatively inexpensive scan of your IT system to determine its vulnerabilities, educating your staff about the threat of social engineering, and keeping up with security fixes.

And, since hackers aren’t the only ones breaking into databases (disgruntled employees and those experiencing tough financial times are other threats), it’s smart for CFOs to insist upon background checks for new employees and the implementation of strict data-access rules, such as making sure HR can’t access customer data and sales can’t access employee data.

Other relatively low-cost measures include mandating strong passwords (at least eight characters, a mix of numerals and upper- and lower-case letters). Customer data should be kept off of laptops, smart phones, and USB drives unless encrypted or, at least, password protected. Also, it’s not smart to store unneeded data; erase it.

Finally, consider buying cyber insurance. The cost has come down by more than 20% from five years ago, according to Robert Parisi, senior vice president of insurance broker Marsh. Plus, he says, insurers are tossing in freebies such as security assessments, victim breach notification, and credit monitoring.

“In an era where a lot of companies have cut into IT resources, insurance can be as important as the firewall,” Ponemon says. “With cyber insurance,” ACE’s Merrill adds, sounding like a salesman, “you’re buying more than coverage; you’re buying peace of mind.”

CFO Summary

- Hackers seeking personally identifiable information (PID) often target midsize companies.
- Midsize businesses with up to 100 employees and $100 million a year in revenue are especially at risk for security breaches.
- “Phishing,” or social engineering, has caused more breaches than all external attacks combined.
- SMBs can remain protected without a high expense by scanning IT systems for vulnerability, by making employees aware of risks, and by maintaining the security system.
WIPING THE SLATE CLEAN: DIGITAL COPIER DANGER

Digital copiers pose security risks that companies may not appreciate, especially smaller firms without dedicated information-security staff. But what the greatest threat is, and how high the relative risk levels are, are matters of current debate.

The issue has received a lot of attention since 2010, when the CBS Evening News ran a report on it. CBS declined to say how much traffic its video report has generated on its own Website, but the network also posted the report on YouTube, where it has received almost 1 million views, and the blogosphere has not stopped buzzing about the topic.

Most business copiers today have hard drives on which images of copied or scanned pages are stored. Most copiers are leased, and after lease terms expire, leasing companies often unload the used machines to wholesale resellers. If a company doesn’t wipe the hard drive clean before returning a copier, its contents—which could include sensitive employee or customer information—could be exposed to identity thieves. The same applies to copiers that a company owns and tries to sell.

As reported by CBS, John Juntunen, founder of Digital Copier Security, a company that markets a 10-step process for cleansing copiers, accompanied reporters to a warehouse where they randomly bought four machines for roughly $300 each. All four copiers had unwiped hard drives. Two had been leased by the police department in Buffalo, New York, and one had been leased by an unidentified small construction company. The fourth copier came from Affinity Insurance, a health-care–services provider to low-income residents in the New York City area. It contained 300 pages of individuals’ medical records.

“It’s very important that CFOs and their IT staffs take stock of the individual machines they have and what level of risk there really is,” Juntunen tells CFO. Simply pulling out the hard drive is not an option except for copiers that a company owns and plans to junk, he adds, because in most cases the hard drive contains the operating code that makes the machine run.

Juntunen notes, though, that CBS erred in saying that copier hard drives store images of every scanned and copied document. Rather, storage space is finite, and after capacity is reached, older images are overwritten. The number of documents that copiers hold varies widely and depends on the make and model, he adds.

If a company doesn’t wipe the hard drive clean before returning a copier, its contents—which could include sensitive employee or customer information—could be exposed to identity thieves. The same applies to copiers that a company owns and tries to sell.

In fact, for that reason, the degree of risk as depicted in the CBS report may be overblown for any particular company, says Mike Rossander, a security expert who works for Westfield Group, a Midwest regional insurer. Images are large, and copiers with 40 gigabyte hard drives, such as the HP 4000 series machines that Westfield uses, fill up fast.

“A high-use copier might have images that are
CFO Summary

- Digital copiers pose security threats as images of copied or scanned pages may be stored on their hard drives.
- Identity thieves may have access to sensitive information if companies do not wipe the copiers’ hard drives before returning them to leasing companies or wholesale retailers.
- The FTC has acknowledged the risks in copiers and is reaching out to manufacturers and supply stores to alert them of privacy issues.
- To reduce risk when disposing or ending a lease, either wipe the hard drive or scan non-sensitive pages to overwrite the hard drive.
While the lure of financial savings has quickly driven the use of cloud-computing service in the corporate sphere, not many senior executives have really examined the risks of using the cloud or how to deal with them. Adding to the problem is that it has been hard to identify exposures and obtain adequate insurance coverage for the risk, experts agree. Much of the risk has its origin in the increasing use of cloud-computing services. The 2012 Cisco Global Cloud Networking survey of 1,300 information-technology executives from 13 countries found that by the end of 2012, 20% of companies were using cloud-computing technology to deliver most of the software applications used by their businesses. Easy targets, because IT isn’t a core part of their company’s functions, nontech executives at nontech companies are often being “aggressively encouraged” to use cloud solutions, Lori S. Nugent, co-chair of data security and cyber liability with Wilson Elser Moskowitz Edelman & Dicker LLP in Chicago, notes. In particular, CFOs are being encouraged to outsource IT, often saddling their companies with a hard cost that tends to increase and complicate security issues. “It sounds easier to just let somebody else worry about that,” she says. “By going to cloud, the theory is that you can outsource all of that and that it’s more scalable, because you can increase or decrease the scope of service you have.” The reality, however, is there are “substantial costs associated with moving to cloud” via outsourcing, she says. “It doesn’t mean you shouldn’t do it, it just means you have to be protected for those exposures—if there is a breach at the cloud itself.” To be sure, mid- and small-size companies may not have the resources or focus to do IT well themselves, she says. “In that situation, going to [the] cloud can be smart, because you can get better IT services than you would otherwise be able to afford.” Nugent adds, however, that “the bottom line is cloudier than is currently perceived when evaluating cloud.” When moving over to the cloud, it’s important not to presume that there will be no IT issues to be concerned about. A solution that may be effective, she says, is to “put some things in the cloud, but not everything.” She would be very reluctant, for example, to put sensitive intellectual property or research and development information on the cloud, which is a “shared environment.” She also notes that CFOs would be wise to document the rationale for any decisions made to put sensitive information on the cloud. “It’s not a question of if there will be a breach, it’s when,” she says.
Nugent says strong coverage is now being offered at “fairly inexpensive cost” for cyber risks. A number of these policies include coverage for a company’s data that is held by vendors, such as one that does billing, she notes. Insurers include Lloyd’s and U.S. and European companies.

Fewer than 20% of companies are purchasing the coverage, she adds, and advises CFOs to work with their risk managers and insurance brokers familiar with the cloud to identify and mitigate the risks. In the case of a data breach, she says, many policies respond to the breach costs, forensics, and other expenses. They also cover regulatory fines and penalties, as well as litigation costs, and a number also provide coverage for public-relations services to address bad publicity surrounding a breach.

Robert Parisi, network security and privacy practices leader for Marsh, a big insurance brokerage, points out that a danger to some companies is that they may be using cloud services “so far down the food chain that they might not be entirely aware of it.”

The risk may simply involve executives having access to a cloud service provided by an outside vendor when they’re traveling, he says. Problems may stem from how the person gains access to the service—from an unsecure Wi-Fi connection in an unsecure physical location, for instance.

Other sources of corporate risk include outsourced payment-processing systems, actuarial tables, and credit confirmation. Parisi points out three reasons breaches may occur:

• A third party now has control over an element of the company’s operations/infrastructure.
• A third party may be connecting into the network either actively by reaching into it or passively, as when the company reaches out to a cloud provider that may itself be vulnerable.
• By accessing certain programs through the cloud, an organization’s IT staff may not have fully ramped up their understanding of the program to the same extent that it would have had the company hosted it internally.

Traditional property-insurance policies typically cover the loss and the extra expense associated with a business interruption only if the functioning of the company’s own property—in this case, computer systems—is interrupted.

What’s missing in this coverage is loss of income stemming from an interruption of outsourced services, costs incurred in procuring the services of a new cloud provider, and the costs of transitioning to a new provider. Costs incurred include the transition of software and data to the new provider, Parisi explains.

Ron Cooley, director of risk management for W.W. Grainger Inc., an industrial supply company, says his company uses multiple cloud services but does not have a specific cloud-coverage policy. “The challenge is that a lot of these policies are evolving because technology is moving so quickly,” he adds, noting that the exposures can also be much larger than the coverage available.

**CFO Summary**

- Make sure you understand how secure your cloud-computing services really are.
- CFOs are often encouraged to outsource IT, but this leads to threats of exposure in the Cloud.
- CFOs should consider purchasing coverage for data plans to protect against cyber risks.

Sources for Risky Business: SMB Vulnerability:
“Compliance does not equal security. Certain applications have to pass SOX testing, but hackers won’t use those. Locking the front and back doors is important, but it’s no good locking them and leaving the windows open. Compliance focuses on a few doors and IT, focuses on what compliance requires. CFOs, must think beyond that.”
IN THE DARK: DENIAL OF SERVICE

No one likes being awakened in the middle of the night. It’s never good news. And it wasn’t good news shortly after midnight on July 21, 2011, when Yola president and chief operating officer Trevor Harries-Jones was yanked from sleep by the phone ringing in his San Francisco bedroom.

Yola is a global, do-it-yourself website-building-and-hosting service with more than 6 million mainly small business customers depending upon the company to keep their sites, Facebook pages, e-mail systems, and online stores up and running. The call that woke Harries-Jones came from his head of engineering, based in Cape Town, South Africa.

“She said we were down,” he recalls. “It was a massive distributed denial of service (DDoS) attack.”

The engineer told him she was doing all she could. Harries-Jones grabbed a few more hours of sleep and then went to the office, where he spent most of the day updating customers, trying to assure them that Yola was doing all it could to get their sites back up, and talking to Yola’s third-party hosting provider, which was trying—unsuccessfully—to get Yola back online.

This wasn’t the first time Yola had experienced a DDoS, but it was the worst. For eight hours, Yola-hosted customer sites were inoperable. Mission-critical operations were disrupted. E-commerce sites couldn’t do business. Revenue was lost.
Professional sites were inaccessible. Potential clients went elsewhere. All of Yola’s customers across all time zones and geographies were affected. Yola itself was isolated, its customer–support forum down.

Why was Yola attacked? “You look across the Internet,” Harries-Jones says, “and it’s happening all the time. Does it come from our competition? Is somebody unhappy with us because we haven’t allowed them on our platform? We manage the content of websites we host, and sometimes we have to take them down.”

Rarely does one ever find out why one is attacked. “We didn’t receive a ransom note,” says Harries-Jones.

“Attacks have become more and more sophisticated over time,” he explains. The majority of incidents Yola had experienced prior to 2011 were simple denial of service (DoS) attacks, which means they came from a single point. That, says Harries-Jones, made them “easier to isolate and cut out of the stream.” And they were something Yola, or its providers, could deal with internally. DDoS attacks, however, come from everywhere and use thousands of computers, all sending requests to Yola’s servers at the same time, making it impossible to determine legitimate from ill-intentioned traffic, and eventually overwhelming the network and crashing it.

“You’re seeing more and more of these [DDoS-type] attacks,” says Harries-Jones, “and they’re becoming more frequent.” (In February 2012, Nasdaq suffered a DoS attack that, while not affecting trades, blocked access to the exchange’s corporate website.)

Yola couldn’t deal with last summer’s attack by itself. And, as Harries-Jones says, “This was a driver to get us professional help, to outsource.” He got the name of a security firm from one of his Internet Service Providers (ISPs). He made the call. “Our site is down,” he said. “Can you help us?”

Why Anyone Can Take You Down

According to data collected by Panda Security, 50% of all computers scanned around the globe in January 2012 were infected with malware—malicious software code designed to steal data, gain access to computer systems, or take control of machines without the computers’ owners knowing it, turning them into “zombies” or “bots.” Once a computer becomes a zombie, it can be used as a platform for launching DDoS attacks.

Anyone can do it.

“It’s easy to obtain tools, scripts, products for hacker or breach activity,” says Gary Loveland, a principal in PricewaterhouseCoopers’s security practice. Anyone can go on the Internet and rent a botnet, a network of infected computers that can be remotely controlled.

“No one can handle a DDoS by himself. DDoS requires cooperation. That means the Internet service providers, the telecommunications providers, the federal government. DDoS requires a coordinated response.”

“You pay by the number of bots you want,” says Paul Sop, chief technology officer at Prolexic, a security company dedicated to combating DDoS attacks and the firm Yola’s Harries-Jones called for help. “You can get 50 or you can get 50,000. Or more.” Prolexic, Sop says, has fought up to half-a-million computers at one time.

Once all those zombies are connected to a command-and-control server, you’re ready to launch your own DDoS attack. Must you worry about getting caught?

“And anyone can install the Onion Router (TOR) that will shield your identity,” Sop says, explaining how TOR will bounce a request—say to Google—from your computer to someplace in Africa and then to somewhere in Asia and then to a third, fourth, or fifth node before it gets to Google, thereby making it almost impossible to trace the IP address of your machine. “Whoever is launching the attack,” says Sop, “it’s the infected bots doing the attacking. They’re controlled by the command-and-control server. And behind that, there may be someone further hidden, the puppet master, talking to the command-and-control server.”

No one, Sop asserts, can handle a DDoS by himself. Loveland agrees. “DDoS requires cooperation,” he says. “That means the Internet service providers, the telecommunications providers, the federal government. DDoS requires a coordinated response.”

Could you be a target for a DDoS attack? Read Cyber-Attacks: Computer Says No.
Answering a Call for Help

When Prolexic got the call from Yola, it was, in Prolexic’s terminology, “a hot call” for immediate assistance. And because Yola was not a client, there was an emergency fee. “First,” says Sop, “we get the paperwork right. We don’t do this for free. Our pricing, a monthly fee, is determined by your bandwidth and your risk. We have to know who we’re protecting, a giant global media company or a smaller business. Then we hit the ground running. “We work with the customer’s team to change its network configurations, to route its traffic to us. All the traffic, good and bad, comes through us. Our job is to pass through the good, filter out the bad. It takes software and hardware and people who take care of the event. All the software in the world won’t help if you don’t have people with the right skills.”

DDoS, Sop hastens to emphasize, is not like spam. “There’s an adversary out there,” he says. “A human mind with a desire to punish. People often don’t understand that the attack is a campaign. The nature of attack vectors changes. People underestimate the variations of the attack. It starts with something that perhaps the ISP can handle. The next day, it’s entirely changed and then it changes again.”

The situation “is asymmetric warfare. The attacker has so much more capacity than the attackee. We level the field. It’s like playing chess. We play until we win or it’s a stalemate, meaning they give up.”

“Be sure your hosting provider has a DDoS mitigation strategy,” suggests Yola’s Harries-Jones, who says that although Yola has been the target of similar attacks since signing on with Prolexic, his company suffered no service interruptions. For Yola, uptime is the critical business risk that needs to be managed.

Many organizations, Loveland says, believe that because they are Sarbanes-Oxley or HIPAA compliant, they’re secure. But compliance, he says, does not equal security. “Certain applications have to pass SOX testing, but hackers won’t use those. Locking the front and back doors is important, but it’s no good locking them and leaving the windows open. Compliance focuses on a few doors and IT focuses on what compliance requires.” CFOs, Loveland believes, must think beyond that.

CFO Summary

- In 2011, Yola, a DIY website-building service, suffered from a distributed denial of service (DDoS) attack.
- Investigate if your hosting provider has a DDoS mitigation strategy.
- Malicious software may be easily obtained and used to steal data, gain access to computer systems, or take control of machines. Recognize the risks your enterprise is taking.
Frank Abagnale, the ex–con man made famous in the Hollywood movie *Catch Me If You Can*, is known more for how he committed fraud than how he prevents it. But small businesses can learn a thing or two about preventing check fraud from the now–respected consultant who frequently works with the FBI.

Although businesses are increasingly becoming more paperless, Abagnale said on an American Institute of Certified Public Accountants’s (AICPA) webcast, and despite the technological mobile-payment advancements available today, business check use has decreased only slightly during the past 10 years (though individual check use has decreased by a far greater amount). What’s more, he noted, most payments made by one company to another are still made by checks. He conceded, however, that younger adults use checks much less often for both business and individual reasons.

That’s a harsh reality for small businesses trying to prevent fraud, he said. Abagnale spent his youth scamming corporations with fake corporate checks. But a new kind of check fraud now links old-fashioned check cashing with fast mobile-payment technology. “We now have a crime wave going on,” he said. “What is happening is, I get a check from you . . . scan it onto my iPhone in my account, and go cash it somewhere else. I’ve cashed it twice.”

This kind of fraud can particularly hurt small businesses today, he says, since many bookkeeping and accounting functions are outsourced, and busy company executives are not always even aware a check to a vendor has been cashed twice, for example.

Smaller companies are also not always up on the latest antifraud printers used to make and disseminate those checks to begin with, Abagnale said. “If you are not using the proper ribbon, the ink can come off. You want to make sure you are using security ribbon made of ink.” One can cut down on fraud simply by choosing the right printer, whether matrix or laser, for one’s particular kind of business. That’s because some logos and corporate graphics can be scanned more easily in some kinds of printers than others.

Having the right business equipment, he said, should help small and large businesses cut down on both external fraud and insider fraud—those actions perpetrated by a company’s own employees. He should know. He claims that before becoming an FBI consultant and fraud–prevention expert, he forged more than $2.5 million in bogus checks and infiltrated dozens of corporations.

“We now have a crime wave going on. “What is happening is, I get a check from you . . . scan it onto my iPhone in my account, and go cash it somewhere else. I’ve cashed it twice.”

**Inside Job**

Insider fraud indeed is a major concern for CFOs, CEOs, and other senior executives at both small and large companies, according to a recent AICPA forensic and valuation services survey. For the study, the AICPA interviewed 737 respondents at firms with 100 or fewer accounting professionals.

The highest number of survey participants (38%) expected financial fraud committed wholly by company personnel to increase the most in the next two to five years compared with outside fraud. The next-highest portion of respondents (34%) believed that company personnel along with the involvement of third parties (outside businesses the...
company does business with) would be responsible for an increase in fraud. Another 18% expected no change in fraud, while 10% saw an increase in fraud committed entirely by third parties.

Embezzlement or misappropriation of company funds, which is typically associated with insider fraud, was also flagged in the AICPA survey as an area to watch in the coming years. More than 50% of the respondents said increases in embezzlement would most likely involve company personnel on their own. In contrast, more than 30% believed it would involve company personnel working with third parties and 17% expected no change.

Similarly, 53% said they expected an increase in corrupt practices involving company personnel working with third parties during the next two to five years, while 27% expected an increase involving company personnel working alone. Only 20% believed there would be an increase in fraud involving third parties working alone.

What kinds of fraud are looming on the horizon? The highest percentage of respondents to the AICPA survey (23%) expected most fraud cases in the next two to five years would involve contract breaches, while 17% believed most cases would involve business torts.

For Rodney Hurd, CFO of Bridgeway Capital Advisors, a financial advisory specializing in lease and debt financings, it is precisely the contracts or undisclosed agreements performed by corporate insiders that can cause the thorniest problems for both small and large-company CFOs. For example, side letters, those promotional sales letters put out by corporate marketing/sales departments or other internal units that often offer a special sales incentive apart from what the company typically offers, can have significant repercussions, he says.

Too often, employees structure such transactions favorably to a customer just to get a deal. That may be the first time accounting or even the CFO hears about the financial arrangement. Such employees “are just working out the deals themselves without running [them] through accounting. I’ve been around people being terminated as a result of that. This is a very delicate position: to promote a ‘can do’ culture while not tolerating ‘can’t dos,” he says.

Keeping one step ahead of corporate fraud, though, starts in all levels within a firm, not just senior management, notes Hurd. Good fraud monitoring should begin with training employees just starting out in a company. But he offers one word of advice: “If you observe a pronounced change in your employer’s risk taking and transparency, then you generally should get out of there.”

The same advice can be applied to CFOs. “The other side of the coin is you have to be aware of what’s going on as a financial officer,” says Hurd. “You have to be seen as a person who is there to try and make things happen.”

Richard Sibery, partner in fraud investigation and dispute services at Ernst & Young, agrees. He says there is an increased focus today by finance chiefs on monitoring fraud within a corporation. “There was some focus on fraud prevention and protection years ago, but there was little appetite from corporate to look into it too much . . . we’ve seen significant change since then.”

CFOs and senior executives today are “trying to get out there and do specific procedures to monitor for fraud,” he notes. While companies differ on where to place that fraud-monitoring function, he says companies are looking at internal checks and balances. The numbers are telling the same story. The AICPA study found that 24% of the respondents increased the number of internal forensic professionals in their practice.

CFO Summary

- According to Frank Abagnale, an ex-con man, most payments made by one company to another are still made by checks, which are large targets for fraud.
- Because many accounting functions are outsourced, company executives may not notice that a check to a vendor has been cashed twice.
- Strengthen internal controls to prevent fraud by insiders

Sources for Data Breach: The Reality of Cyber Attacks:
“As cyber threats become more pervasive, small businesses—particularly those in the high-technology, financial-services and health-care industries—are taking out insurance policies designed to bolster their protection from the potentially crippling costs that can accompany data breaches and other cyber attacks.”
PLAYING IT SAFE: CYBER-LIABILITY INSURANCE

Telecommunications giant Verizon released its annual investigative report of data breaches in April 2013, which found that small businesses are the number-one target of cyber-espionage attackers.

Almost half of the 621 confirmed data-breach incidents Verizon recorded in 2012 occurred at companies with fewer than 1,000 employees, including 193 incidents at those with fewer than 100 workers. Similarly, security company Symantec reported last week that cyber attacks on businesses with fewer than 250 employees leaped 31 percent in 2012, following an 18 percent climb in 2011. Both reports cited small businesses' inadequate security infrastructure for protecting financial information, customer data and intellectual property.

As cyber threats become more pervasive, small businesses—particularly those in the high-technology, financial-services and health-care industries—are taking out insurance policies designed to bolster their protection from the potentially crippling costs that can accompany data breaches and other cyber attacks.

Ethan Miller, an attorney specializing in trade secrets at international law firm Hogan Lovells, has seen an increasing number of small businesses, especially start-up companies in Silicon Valley, approach insurance brokers about protecting their intellectual property. “Here in Silicon Valley, [a company’s] intellectual property is its lifeblood. Brokers not only issue property and general-liability policies, they also issue policies that specifically provide protection in the event of a hacking or security breach.”

Larger organizations—with 1,000 or more employees—typically have a risk manager that handles their risk and liability, along with a robust IT department that works to reduce the risk of a breach or attack with firewalls and antivirus software. But smaller companies, says Miller, are typically unsophisticated in their data-security methods. They may have only a CFO or chief operating officer that doubles as a risk manager. “They’re not going to have the expertise to put these protections in place up front, and that’s where a good policy can come into play,” he says.

Cyber-liability insurance policies generally cover costs incurred by the loss of trade secrets and intellectual property, known as first-party claims. They also cover damages a company must pay should a customer sue it for lost or compromised personal information, known as a third-party claim. Most policies include business-interruption coverage in the event of a denial-of-service attack, whereby the insurance company would provide payment reimbursement for expenses surrounding such an attack. Such costs, Miller says, “can sometimes be a life-or-death issue for smaller companies.”

Cyber insurance policies also cover the cost of a

Most policies include business-interruption coverage in the event of a denial-of-service attack, whereby the insurance company would provide payment reimbursement for expenses surrounding such an attack.

As cyber threats become more pervasive, small businesses—particularly those in the high-technology, financial-services and health-care industries—are taking out insurance policies designed to bolster their protection from the potentially crippling costs that can accompany data breaches and other cyber attacks.
forensic IT examination of how the breach or data loss occurred. Some even pay for a public relations firm to mitigate negative publicity following a breach, as well as regulatory fines and penalties.

“Crisis management is really critical,” says Miller. “Again, a large corporation would typically have sophisticated crisis management or a consultant on retainer, but a smaller company won’t, and it might not know how to send appropriate notices to customers when there’s been a breach, which is required under law.”

He continues, “The insurance company will have to reduce its risk, so it’s going to consult with customers to make sure they have specific types of protections and policies in place that a risk-management department at a larger company would already be doing.”

Miller stresses that cyber policies are not meant to substitute for diligent, proactive management of cyber security risk, such as sound data-protection protocols and employee education. “And the insurance company is going to demand you take these protections as part of the application, so as a practical matter you can’t become complacent or you’ll violate the policy,” he says.

As with any insurance policy, cyber-liability insurance is primarily about peace of mind. “If you’re a closely held corporation where your founders are often running the company and have the largest financial stake in it, you’re going to want peace of mind that your largest investment is as protected as it can be.”

Smaller health-care providers, which handle massive amounts of personal customer data and must comply with the Health Insurance Portability and Accountability Act (HIPAA) and other regulatory requirements, are particularly vulnerable to cyber threats. A December 2012 study by independent research firm the Ponemon Institute found that 94 percent of health-care organizations surveyed suffered at least one data breach in 2011 and 2012, with 45 percent of the organizations experiencing more than five data breaches during that time. Ponemon estimated the breaches could be costing the U.S. health-care industry an average of $7 billion annually.

Miller urges such organizations, and others that value their data highly, to look into this type of risk transfer. “Any broker worth his salt will, depending on the nature of the business a customer is in, recommend such a policy. Then the company will conduct a cost–benefit analysis.”

He concludes, “More and more often, as security breaches continue to be all over the news, these analyses weigh heavily in favor of cyber insurance. Just as a business would insure a warehouse against fire loss, a lot of companies that do the cost–benefit analysis see that $2,000 to $4,000 per year can protect against a different kind of catastrophic loss.”

**CFO Summary**

- Cyber attacks on businesses with fewer than 250 employees jumped from 18% in 2011 to 31% in 2012.
- An increasing number of small businesses have begun to look into insurance policies that provide protection in the event of a security breach.
- Cyber-liability insurance policies typically cover costs incurred by the loss of trade secrets and intellectual property, third-party claims by customers whose personal information has been compromised, business interruptions, and the costs of a forensic IT examination.
A remote workforce, distributed teams, and the use of contract labor are facts of operational life for almost all small and midsize businesses today. In order to collaborate, these far-flung teams are using a variety of free and paid services (for example, Dropbox, Google Drive, and others) both to share documents and store data. Coupled with the rising bring-your-own-device trend, the diffusion of data across multiple services and multiple devices is posing significant enterprise risk in terms of potential data loss, security breaches, and regulatory compliance to small-businesses CFOs. A 2010 Ponemon Institute study determined that the average cost to a business of each lost laptop was a little more than $40,000. Further, insurance-industry data provider A.M. Best found that 51% of midsize businesses that suffer a catastrophic data loss shutter their doors within two years.

Clearly, without centralized data storage, without enforced policies across multiple locations, employees, and devices, small and midsize businesses are living dangerously.

One way to mitigate risk is to invest in an enterprisewide solution that standardizes on a single tool for centralized document storage. As CFOs go down this path, they will be challenged in three key areas:

There are at least 50 different enterprise cloud storage and backup solutions in the marketplace today.

Options range from premium consumer products, such as Dropbox for Teams, to more traditional enterprise solutions, such as Microsoft’s SharePoint. Consumer-oriented solutions that have been upgraded with security and access control features for corporate use tend to be more user-friendly, and easier to implement than more traditional enterprise software, but lack their sophistication and customization capabilities.
There is a cost trade-off between products that require high setup costs but have low recurring fees and solutions that require minimal setup costs but charge higher recurring fees.

For example, a robust tool like SharePoint has significant upfront setup and configuration costs ($1,000–$14,000 for a 20–50 person firm); however, it has relatively low ongoing costs ($4–$8 per user per month, or a fixed monthly rate for a hosted cloud solution). Conversely, more consumer-oriented solutions such as Box for Business or Dropbox for Teams have low initial setup costs but often have considerably higher recurring costs ($10–$15 per user per month), which can rise quickly as your firm grows and adds staff.

Management must consider the investment required in change management to support the adoption of whatever software you choose.

Most small and even many midsize businesses lack the resources and expertise to train employees in the software’s use and encourage them to adopt it in their work. Consumer solutions, as noted, are built to be easy to use. Therefore, employees will require less training and, perhaps, less encouragement.

To navigate these challenges, and to make this important and complex investment decision, CFOs need to think about the future needs of their organization across a number of dimensions. The degree of anticipated growth, both in staff and data, plus the desirability of making a large capital expenditure versus an operating expense over time, will figure into deciding what type of solution is right for the business.

For slower-growth companies, paying a premium for an easy-to-use, per-user-priced consumer solution makes sense. In these cases, companies should standardize on a single upgraded consumer solution based on employee preferences. (You can poll your employees to identify the most popular tool; chances are many are already using one of these solutions for work and for their personal life.) Another consideration when choosing collaboration software from a nontraditional source is the financial health of the provider. Dropbox for Teams and Box for Business presently are both popular and well-funded.

For fast-growth companies, in which flexibility and the ability to customize can be tied profitably to workflow, investing in a more enterprise-grade solution such as SharePoint or IBM and Oracle’s collaboration offerings may be more cost-effective in the long run, despite the greater upfront cost.

CFOs must include in the higher cost of change management (training and support) in their analysis. At the same time, companies choosing to make the initial investment in an industrial-strength solution should establish clear policies to enforce adoption and discourage the use of alternatives, as IBM did when it banned employees from using Dropbox and iCloud last year. If the company allows its data to sprawl across various document storage and collaboration solutions, the benefits of the enterprise solution can quickly evaporate.

One midsize health-care industry software company, for example, had a geographically dispersed, multidevice workforce that shared content across multiple and disparate databases, servers, and e-mail. Although the company could have benefited from a centralized data-management solution, it did not want to invest in a full-blown IT infrastructure for a firm of just 50 people. Therefore, it chose a consumerized plug-and-play, cloud-based platform for its file auditing, management, searching, and security needs, and so far has been happy with the operational simplicity it has provided for a relatively low capital expenditure.

Finance executives of small and midsize companies should approach the diffusion of data within their organization not only as a risk to be mitigated but also as an opportunity to be seized: to increase collaboration and improve the productivity of the virtual teams that are increasingly becoming the norm in business today.

CFO Summary

- Many SMBs use services like Dropbox and Google Drive to ease collaboration.
- To reduce risk while using online collaboration tools, utilize an enterprise wide system. The level of expected growth in a company may should influence a company’s choice of collaboration software.

Data breaches have a way of being much worse than they initially seem. The infamous theft of customer information from T.J.Maxx in the 2000s turned out to be far more extensive than originally reported, involving more than 45 million credit and debit cards. More recently, the purloining of more than 450,000 user names and passwords from Yahoo in July 2012 also exposed the e-mail addresses of Gmail, AOL, Hotmail, Comcast, MSN, and several other services. If subscribers to the breached Yahoo service used the same passwords for their e-mail accounts, then those passwords are also in the possession of the hacking group that breached Yahoo and posted the names and passwords online.

Not surprisingly, Yahoo came under fire for its security practices and for not informing its customers of the breach faster than it did. At the end of July, a Yahoo user filed a lawsuit (and is seeking class-action status) against the company for failing to safeguard users’ personal information.

But data breaches aren’t just a problem for large outfits like T.J.Maxx and Yahoo. Nearly 72% of breaches in 2011 involved organizations with 100 or fewer employees, according to Verizon’s 2012 Data Breach Investigations Report. For small and midsize businesses that experienced downtime after a breach, the median cost was $12,500 a day, according to a 2011 survey by security provider Symantec.

Unlike large companies, smaller businesses have fewer resources to deal with cybercrime, making them an “ideal target” for “money-driven, risk-averse cybercriminals,” says the Verizon report. What’s more, “small and midsize companies can lose as many records as large ones,” says Larry Ponemon, chairman of the Ponemon Institute, a privacy and data protection research group.

Insurance: Available but Expensive

How can smaller companies protect themselves from cyber loss? Insurance is one way, but historically it’s been costly. “You can always get insurance for anything,” says Ponemon. “But if you go to a specialty insurer, the premiums are high, as it’s difficult to model exposure” in the cyberworld, he says. And that makes underwriting difficult. In particular, the tough part for an underwriter “is finding out where the risk is,” says Steve Vallone, a broker at Worldwide Facilities, a wholesale specialty insurance brokerage.

Some carriers figure out how to charge based on a company’s revenue, says Vallone, “but that doesn’t
bring in the whole picture: how sophisticated your IT is, how up-to-date your systems are, what information you keep on those systems, and whether you keep customer information on file or you give it to third parties." Still, it is getting cheaper to buy coverage as insurers become more familiar with IT security best practices, he adds.

Insurers that offer breach-response services in addition to liability coverage can help prevent small companies from making costly mistakes in responding to data breaches, contends Jamie Orye, who manages an underwriting team at Beazly, a specialty insurer. For instance, after becoming aware of a data breach, companies are often in a rush to send out letters to their affected customers, he says. But “the law identifies what can and can’t be put in a letter,” he notes. “The letters themselves present a risk of violating regulations.”

Without insurance that includes response assistance, says Vallone, “if you [have] a breach, you [have] to hire lawyers; maybe hire an IT consultant to figure out what went wrong and how to fix it. That’s a lot of work. Then you have to consider hiring a PR firm. What do you do? There’s a lot of uncertainty.” Vallone believes cyber- and breach insurance, especially in the small and midsize business space, will become as prominent as employment practices liability insurance, which used to be elective and is now almost universal.

When looking for data-breach insurance in particular, Ponemon suggests asking insurers how many breaches they have handled, whether they have dealt with breaches in the company’s industry, who their vendors are, and whether they insure for third-party data loss.

An Ounce of Prevention

There are also simple steps that small and midsize companies can take to ward off data breaches. According to the Verizon report, 79% of the hacking attacks included were opportunistic rather than targeted. Among the largest companies—those with at least 1,000 employees—that percentage dropped to 35%. In other words, many smaller companies are getting cyber-burgled because they’ve left their front doors wide open. “Targets of opportunity are breached not because of who they are but because of what they’ve presented to the attacker—an open door, a weakness, or a vulnerability that can be easily exploited,” says Marc Spitler, security principal at Verizon and co-author of the report.

For the most part, “the attackers don’t even know who these small businesses are or what they do,” Spitler says. “They’re going after things like payment cards, and it’s really no concern to them where they get them, as long as they get them from somebody.”

Hacking accounted for 81% of data breaches in the Verizon report, and more than half of those breaches were achieved because firms used default or guessable credentials. Thus, one of the simplest ways to avoid an opportunistic data breach is to create stronger passwords (a combination of numbers and upper- and lowercase letters) and change the default credentials and administrative passwords that come with point-of-sale (POS) systems and other devices that access the Internet.

The Verizon report also suggests that companies implement a firewall or access control list on remote access services, avoid using POS systems to browse the Internet, and make sure their POS systems are PCI DSS compliant. “These tips may seem simple,” the report adds, “but all the evidence at our disposal suggests a huge chunk of the problem for smaller businesses would be knocked out if they were widely adopted.”

CFO Summary

• Typically, SMBs have fewer resources to use to protect data and have become targets.
• According to Verizon’s 2012 Data Breach Investigations Report, nearly 72% of cyber breaches in 2011 involved companies with 100 or fewer employees.
• Smaller businesses are often attacked because they’ve left their front doors wide open to hackers.
• Implementing firewalls or access control lists can help protect against breaches.

Sources for How to Be Prepared: Small Business Protection:
“Should You Consider Cyber-Liability Insurance?” Taylor Provost, CFO.com, April 24, 2013. Copyright 2013 © CFO Publishing LLC.
CONCLUSION: SUCCESSFUL SMB SECURITY

The notorious bank robber Willie Sutton is famous for having once said that he robbed banks because “that’s where the money is.” Nowadays, the money is in corporate IT systems, and the robbers are skillful programmers trading machine guns and fast getaway cars for bits and bytes.

Small and medium-sized businesses have become the equivalent of the small town bank—easy to loot because their security is minimum, or so the accepted wisdom goes.

Without maintaining a digital data security system, these cyber-robbers can take full control of an enterprise with ease. The consequences an enterprise would face include expensive reconstruction processes, investigations, and a tainted reputation in the public view. An enterprise filters through and file so many different types of sensitive data each day that it is easy to forget the value of the processed information. Should any amount of data be compromised, be sure that you have a strategy to work from because you can never be certain that all systems are completely secure.

While cyber attacks have been increasing, the risk is more likely to lie within the enterprise itself. Make sure that your enterprise has strong internal controls in place to avoid any potential threats from the inside.

By taking the necessary steps to control internal affairs, to defend against outside attacks, and have a plan in place in case of an attack, your enterprise can continue to grow efficiently and safely.