

# Shining a light on Shadow IT

Are you managing the risks of hidden and unauthorized information technology?

5 factors driving Shadow IT >

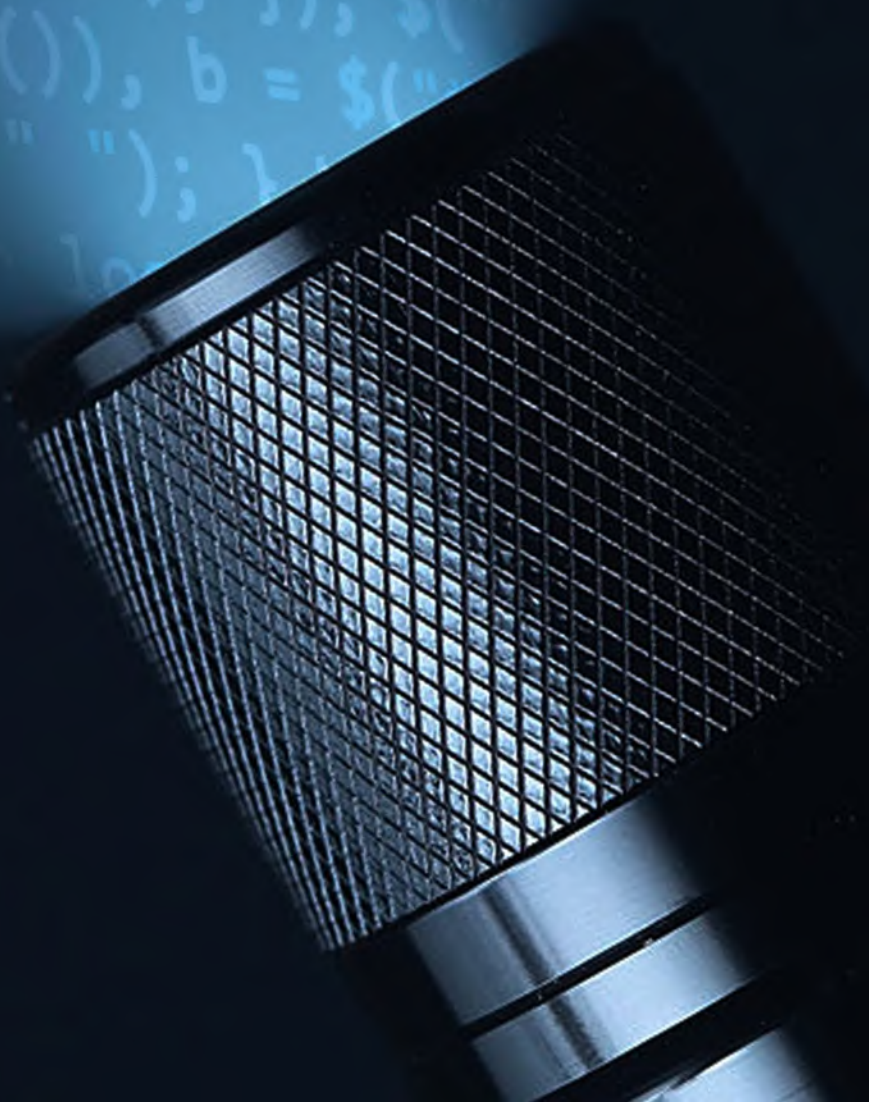
5 Shadow IT practices to shine a light on >

4 key Shadow IT risk categories that  
technology companies should understand >

Minimize exposure to risk categories >

Insurance considerations for Shadow IT >

How Travelers can help >





## A note from Mike Thoma

Managers within technology companies consistently face cost and speed-to-market pressures. These pressures often lead to information technology (IT) projects that are conducted on a “Shadow” basis – out of compliance with official company policies and without oversight from the company’s corporate IT function. Competition gives way to Shadow IT.

Technology companies need to understand that Shadow IT is a favorite playground for hackers and cyber thieves. Right now, Shadow IT may be endangering your intellectual property and sensitive customer or employee data. Before you can take concrete steps to protect your technology business, you must first understand the nature and scope of this risk.

This issue of *Global Technology’s Risk Advisor* shines a light on Shadow IT. First, we describe some of the factors driving the phenomenon. Second, we highlight five of the most important Shadow IT practices for technology companies to understand. Third, we describe the key risk categories and offer several specific ideas for ways to minimize your exposure. With adequate preparation, technology companies can take IT out of the shadows.

### – Mike Thoma

*Practice Lead and Chief Underwriting Officer,  
Travelers Global Technology*

“Technology companies need to understand that Shadow IT is a favorite playground for hackers and cyber thieves.”



#### Important note

The “illustrative risk scenarios” described in this document are intended to facilitate consideration and evaluation of risks, and are not necessarily based on actual events. In addition, these risk scenarios are not a representation that coverage exists or does not exist for any particular claim or loss under any insurance policy or bond sold by Travelers or other carriers. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Some risks may not be insurable. Companies should consult an independent agent or broker to evaluate what coverage is right for them.

The “actions to consider for minimizing risk” described in this document are also intended to facilitate consideration and evaluation of how risks can be mitigated. These are not direct guidance or advice on what actions should be taken. Other actions may be appropriate, depending on the circumstances. Companies should consult an independent agent or broker to evaluate what risk management products or services are right for them.

The reference to any information regarding any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply Travelers endorsement, recommendation or favoring of such item or organization. Any such reference is for informational purposes only. Any potential user of any product identified is expected to conduct their own due diligence and assessment of the vendor, product or service as appropriate for their needs.





## Introduction

Resistance is futile. Shadow IT occurs when users self-select and self-develop technology assets – both hardware and software – without corporate IT’s knowledge or permission. Business leaders find its productivity, affordability and ease-of-use benefits too compelling to ignore. However, this trend hands cyber thieves a golden opportunity.

Many leaders grossly underestimate how big Shadow IT has become. A 2015 Cisco report shows that corporate IT leaders at large enterprises estimated that their companies use an average of 51 cloud services. The actual number turned out to be an eye-popping 730. Even government agencies are not immune. A recent analysis by cloud security firm Skyhigh Networks found an average of 742 cloud services being used by the public sector in the U.S. and Canada – significantly more than their IT departments were aware of.

By providing secure means for managers to use these capabilities and technologies in the workplace, companies can mitigate the dangers of Shadow IT. This way, Chief Information Officers (CIOs) can help their co-workers harness Shadow IT’s power without jeopardizing the corporate systems and data they are responsible for protecting.

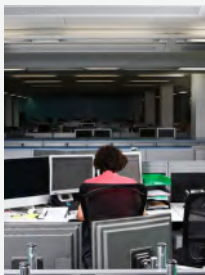
A 2015 Cisco report shows that corporate IT leaders at large enterprises estimated that their companies use an average of 51 cloud services. The actual number turned out to be an eye-popping 730.



## 5 factors driving Shadow IT

In years past, corporate IT has maintained tight control over all enterprise hardware and software. Some of this responsibility is now shifting to nontechnical business managers. Cloud services and personal technologies are now so easy to implement that they can be put to work for the company's benefit with minimal engineering help required.

Even though CIOs cannot stop Shadow IT, they must at least address it. And the first step to getting a handle on this trend is understanding the factors that created Shadow IT in the first place.



### **FACTOR #1: UNDERSTAFFED IT DEPARTMENTS**

Technology companies often struggle with a lack of staffing to meet their needs. This can result from budget pressures, but it is also a product of a scarcity of candidates in the marketplace with adequate software or IT skills. In a survey of the technology industry, IT staffing association TechServe Alliance found that developers with specialized programming language skills were the most difficult to find. The same survey found that technology companies were looking for more personnel with web, mobile and cloud computing skills.

IT professionals highlight information security as one area in which more staffing is sorely needed. In an ISC2 Global Information Security Workforce Study, 62% of respondents indicated that their organizations needed more IT security personnel. Similarly, a survey from the Ponemon Institute found that 77% of IT security and human resources specialists believe that their organizations do not have enough IT security staff.



### **FACTOR #2: BUREAUCRATIC APPROVALS PROCESS**

Business managers are anxious to put their hardware and services budgets to work. However, if they stay within the confines of their own corporation, many face long, slow corporate IT approval processes. A 2015 research study by the Business Performance Innovation (BPI) Network showed that 44% of business and technology managers cited gaining consensus and support for new technology investments as one of the biggest challenges they face. Similarly, an eMarketer survey showed that just 15.5% of marketers were allowed to spend freely on business software. Over 27% indicated that all purchases were heavily scrutinized, and more than one-fifth required approval to spend as little as \$1,000.

The bureaucracy involved in the approvals process is a double-edged sword. On one hand, thorough analysis benefits the corporation by reducing the risk of an unwise purchase. On the other, it prevents the business from being as agile as the marketplace requires. More and more managers choose to bypass the approvals process altogether in favor of Shadow IT. It's quicker and it cuts through the red tape that would otherwise stifle the business innovation they are seeking to generate.



### **FACTOR #3: THE RISE OF SHADOW APPLICATION DEVELOPMENT**

Business unit managers need custom applications written to meet key business needs. But because their official corporate programmers are often backlogged, they sometimes look for application developers elsewhere. They usually find them in two popular Shadow IT sources: “citizen developers” within their own department and external software development firms.

Technology companies often employ people with programming knowledge in functions outside of their corporate IT and software development departments. Co-workers often turn to these people for help when faced with difficult technology questions or obscure error messages. Many are aspiring programmers looking for an opportunity to change careers. And with so many free and low-cost resources available online, they can teach themselves how to program using open source tools like Java, MySQL and Eclipse. So when their business unit managers become frustrated with long IT development turnaround times, these “citizen developers” are often happy to fill the void.

Likewise, business unit managers might choose to hire external development firms. These companies give them shorter development cycles and more personalized service than corporate IT. The challenge with both of these forms of shadow application development, however, is security. Managers who want business benefits like quick time to value and reduced cost might not emphasize security, privacy and compliance features enough, as they feel these features would slow down development.



### **FACTOR #4: EVERYTHING-AS-A-SERVICE**

Most cloud vendors offer Infrastructure-as-a-Service (IaaS) in which the vendor hosts hardware, software and disk space for use over the internet for a flexible per-usage fee. Software-as-a-Service (SaaS) extends the concept by offering complete working applications on an on-demand basis via web services and service-oriented architecture. Many vendors have expanded their cloud services even further to include platform, storage, desktop and disaster recovery, prompting technology thought leaders to describe these offerings as Everything-as-a-Service (XaaS).

These technological benefits translate into one business benefit that managers find irresistible: faster time to market. Managers who must respond to a drastic business change can call their favorite cloud vendor and have a complete server ready to use in as little as a few minutes. Because cloud providers have perfected the art of infrastructure provisioning, they have become the perfect Shadow IT option when new infrastructure is needed.



### **FACTOR #5: BYOD (BRING YOUR OWN DEVICE)**

Almost everyone is attached to their mobile devices, and for many, personal mobile devices are used at work every day. Top management likes the BYOD trend. It shifts the cost of voice and mobile data services from the company to the employee, saving as much as \$80 per user per month – a cost many workers are happy to pay. And because BYOD tends to ride the leading edge of technological capability, the enterprise gets the latest mobile productivity features at no extra charge.

IT leaders, on the other hand, are far more concerned with security and governance than convenience and coolness. However, those who try to force workers to stay within approved boundaries may find themselves fighting a losing battle. When network response times rise to inconveniently high levels, employees quickly reach for their phones and tablets as handy (and often more powerful) desktop alternatives. That's when BYOD morphs into Shadow IT.

# 5 Shadow IT practices to shine a light on

---



Only when Shadow IT comes out of the darkness can IT security professionals hope to fulfill their mission of securing company data. Understandably, companies cannot defend against threats they cannot see. In fact, studies show that a mere 8% of IT leaders worldwide have any meaningful visibility into their companies' Shadow IT usage at all.

Technology companies should understand the following five security threats that can greatly increase the probability of a catastrophic security event. These dangers need to be taken out of the shadows and brought into the open, where they can be managed and minimized.

1

## **PRACTICE #1: SUBSTANDARD DEVELOPMENT TECHNIQUES**

---

When business unit managers order a shadow development project, they are essentially putting themselves in the position of evaluating the programming effort – not just for functionality, but for security. Unlike simple cloud provisioning, evaluating an application development effort requires a good working knowledge of software architecture, design patterns and the latest secure programming techniques – skills few nontechnical managers have.

Internal developers may put their firm's intellectual property at risk if they don't keep up with the latest secure programming techniques. Because programming computers may be an ancillary skill for them, they run the risk that their code will lack security. Because internal employees have fewer obstacles to accessing sensitive data, any vulnerability in their code could lead to loss in the event of a compromise.

Technology industry managers engaged in shadow application development are potentially operating at a dangerous knowledge deficit. If a project comes back from developers with security problems (accidental or intentional), managers may deploy them to production servers without realizing that they are putting their company at risk.

2

## **PRACTICE #2: OVERRELIANCE ON SHADOW CLOUD PROVIDER SECURITY**

---

A 2015 report by Security-as-a-Service firm Alert Logic shows that online criminals are focusing more of their efforts on public clouds. "Hackers, like everyone else, have a limited amount of time to complete their 'job,'" according to the report. "They want to invest their time and resources into attacks that will bear the most fruit: Businesses using cloud environments are largely considered that fruit-bearing jackpot."

Technology business leaders sometimes mistakenly assume that cloud providers automatically handle all of their security needs. But security is a shared responsibility; the cloud buyer must educate himself and his teams on how to use the new infrastructure securely. Sadly, many convenient cloud security features go unactivated because the Shadow IT buyer doesn't take the time to learn how to use them.



### 3

#### **PRACTICE #3: UNSECURED SHADOW FILE STORAGE**

---

Because email is a favorite target of malware developers, network administrators routinely prevent executable and large files from being sent through corporate email servers. In response to these restrictions, employees simply create personal accounts on cloud file-sharing platforms such as Box, Dropbox, iCloud and Google Drive. The cost of these services is small. Low prices make file-sharing services like these a ubiquitous form of Shadow IT simply because almost any employee, regardless of pay level, can afford them.

Once users obtain one of these accounts, they can easily copy files to their personal cloud space to work on them from home. But the very thing that makes these services so convenient also makes them a threat. Many users feel that their files are inherently safe simply because a password is required to access them. As a result, they fail to take even the most basic of security precautions when using these services.

For instance, employees might store files in their personal cloud space that contain unencrypted personally identifiable information (PII). Hospital employees who have done this with protected health information (PHI) may unknowingly violate HIPAA laws. Even those who take the time to encrypt such files often carelessly store the encryption key file in the same directory, making decryption very simple. And because the services are private, the data flowing into and out of them can't be monitored or audited. This means that in the event of a breach, administrators have no way to be sure which data items have been compromised.

### 4

#### **PRACTICE #4: UNSECURED SHADOW MOBILITY**

---

Nearly every technology industry employee has at least one smartphone or tablet. As long as employees limit their use to personal calls and note-taking, the mobile devices pose few threats. But when employees access corporate systems and data on their personal mobile devices with no security controls in place, they cross the line into unsecured shadow mobility.

One of the biggest ways mobile devices threaten corporate data is through synchronization between secured and unsecured devices. Out of convenience, users routinely copy corporate contacts, email and calendar data to their smartphones and then synchronize them with their home computers, which are inherently less secure. Synchronizing unsecured tablets creates yet a different attack point for a skilled cyber thief.

Because mobile devices are easy to carry, they are also easy to lose. An Ernst & Young research study shows that approximately 22% of all mobile devices will be lost or stolen. Fifty percent will never be recovered. If only default security configurations are enabled, it won't take a skilled hacker long to capture and profit from unencrypted corporate data if an IT department cannot wipe the device remotely.

Perhaps the biggest unsecured shadow mobility threat comes from employees' own risky behavior. Executive leaders can be some of the biggest targets for hackers. A 2014 Stroz Friedberg survey showed that 58% of senior managers have accidentally shared sensitive information with the wrong person at least once. Further, an SC Magazine research study revealed that 33% of Fortune 500 corporate executives fell for simple phishing emails such as electronic faxes, fake conference registrations and bogus social media password resets.

While personal mobile devices create significant convenience and even cost savings for corporate enterprises, they also bring security risks.

### 5

#### **PRACTICE #5: USE OF PRE-HACKED SHADOW USB DRIVES**

---

Unlike smartphones and tablets, thumb drives don't have an onboard central processing unit (CPU). However, that doesn't make them any less dangerous to corporate data and systems. All USB memory sticks have firmware – embedded software that tells the device what to do when connected to a USB port. Yet, to save costs, many of the makers of these devices do not protect the firmware, making this seemingly harmless form of Shadow IT particularly insidious.

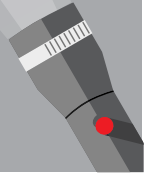
Two German security researchers have created “BadUSB,” a weaponized thumb drive whose firmware tricks its host into thinking the device is a USB-compliant keyboard. Once inserted into a company PC, it rapidly sends a sequence of commands to take control of the machine, giving it full administrator privileges. Thieves with knowledge of company directory structures can program the device to capture and send untold amounts of company data wherever they want within seconds.

The really bad news is that there are no known defenses for these types of USB attacks. Malware scanning software like Norton and McAfee can't detect the problem because they can't access any USB firmware. And since the attacking software's behavior looks just like that of a regular device, its existence won't show up on any security logs.

# 4 key Shadow IT risk categories that technology companies should understand

The more employees use technology at home and in the workplace, the more comfortable they feel making Shadow IT decisions within the context of their jobs. In many cases, comfort levels are unfounded in light of the risks they create.

As a result of Shadow IT practices, technology companies face the four key risk categories described below. Chief Technology Officers (CTOs), or whoever is responsible for IT security, should understand how to recognize these risks so they can evaluate the most effective and efficient ways to control them.



## RISKS

## SOLUTIONS

### Category 1: Bodily injury risk

The Internet of Things (IoT) is not immune to the security risks inherent in Shadow IT. Shop floor operations in manufacturing companies often feature programmable robotics for more efficient assembly operations. These machines are connected to company networks as well, making them every bit as susceptible to malicious attacks as other conventionally recognized network nodes. Should a virus or vector attack assume control of robotic arms when employees are in the area, the company could be liable for bodily injury risk.

#### ILLUSTRATIVE BODILY INJURY RISK SCENARIO

- **City social engineering.** A municipal employee uses real-time technical support via a browser-based chat window on his personal PC, which he brings to work. His PC isn't a member of the network, so his security protection is significantly lower than his work computer. A hacker intercepts his chat window, impersonates tech support and encourages him to divulge sensitive credentials (social engineering). The hacker then uses the captured credentials to breach the city's traffic control system, causing accidents and injuries.





## Category 2: Technology errors and omissions risk

Despite a company's best efforts to safeguard systems, uncontrolled Shadow IT can cause a multitude of problems. A company can be held liable for causing economic loss to others as a result of failure to take reasonable security precautions. It can also stem from a failure of security systems to work as intended due to an error, omission or negligent act.

These factors can impact business continuity, reputation and revenue, depending on the magnitude of the breach. Companies who understand the unique nature of this risk category can better protect themselves from liability claims that arise from Shadow IT.

### ILLUSTRATIVE TECHNOLOGY ERRORS AND OMISSIONS RISK SCENARIOS

- **Failure to test.** A technology company with tried-and-true, mature technology was a leader in its niche. The software product had been stable and error-free for many years, so it was no longer tested and updated. Then one day a company software engineer thought he saw an opportunity to improve the software, and independently made changes without permission. To make matters worse, he did so without testing the code, and the software continued to be delivered to customers. The code failed, leaving customers unable to operate their businesses. Litigation ensued, and the damage claims were substantial.
- **Software not fit for intended use.** A company's software application developer/systems implementer was hired to integrate its technology with a client's HR and payroll system. The work fell behind schedule and the client threatened to fire the company. In an attempt to get the project back on track and to be recognized for solving the problem, a junior software engineer organized a secret team to work extra hours. Suddenly the project was back on schedule and was delivered. Unfortunately, in their efforts to get the project on track quickly, the secret team used open-source code that included unrecognized flaws, and the client's payroll system paid its employees more than they earned. The client ended up firing the developer/systems implementer and filing suit to recover the overpayments.
- **Flawed code.** A product manager at a medical diagnostic equipment manufacturer needed an update to a web interface for one of the manufacturer's most popular medical instruments, but the IT team did not have an available programmer. Thinking he was being helpful and without involvement from IT, the manager hired an external software company for the work. Unfortunately, the external firm did not understand the importance of the level of precision the web interface required, and coded formulas that rounded the calculations from four decimals to two. The web interface was implemented with this flaw in the code, resulting in inaccurate readings. No one was hurt, but a number of medical testing labs lost business over the matter, and several of them sued the equipment manufacturer for financial loss.



## Category 3: Cyber risk

Cyber risk is often defined as the risk of financial loss, business interruption or damage to a company's reputation due to failure to properly secure data it houses within its information systems. Cyber risk can occur as a result of a criminal attack, substandard IT policy, security software failure, or even through the actions of a disgruntled employee.

Cyber risk is a growing concern for organizations across all sectors, and with good reason. The economic damage from data breaches can be catastrophic. A 2015 Ponemon Institute study of large organizations found a mean annualized cyber crime cost of \$7.7 million per year per organization, with costs rising as high as \$65 million per organization.

### ILLUSTRATIVE CYBER RISK SCENARIOS

- **Untrained team member.** A marketing team member happens to have some programming training. His manager asks him to program an ad-hoc web app for customers and resellers because IT is backlogged. Because he has no formal development training, he unknowingly programs security holes into the app. Hackers exploit the vulnerabilities, stealing credit card names and numbers. The company is sued for not adequately protecting sensitive data.
- **Trojan malware-infected thumb drive.** An e-commerce retailer employee uses a USB drive at work to transport large files that would otherwise be stopped by company email. The spreadsheet files contain customer names and credit card numbers. She inserts the drive into her home PC, which is infected with Trojan malware, then brings the same drive to work the next day. The malware infects her work computer and forwards sensitive information to a hacker group that makes fraudulent purchases from the same online retailer using the stolen credit card names and numbers. The company is sued, and loses credibility with its e-commerce customer base.
- **Non-encryption violation.** A hospital employee needs to work from home due to a family commitment. His job requires access to patient data, so he copies the results of several database queries, including sensitive health data, to spreadsheets. He then uploads them to his personal Dropbox account but fails to encrypt them. An annual IT regulatory audit uncovers his actions and reports the data transfer as a violation of HIPAA. The hospital is fined by a regulatory agency and is required to buy and install extra compliance software throughout the entire organization, as well as undergo extensive remedial security training.



## Category 4: Extra expenses

In today's data-driven world where sensitive information is stored and transferred on an increasing number of modes of electronic media, organizations of all sizes are vulnerable to costly and damaging liabilities from unsecured Shadow IT practices.

Whether a Shadow IT buyer is taken advantage of by a hacker, virus or data thief, breaches can have costly side effects. Cleanup costs can mushroom beyond expectation in the event of a breach; companies must find the cause of the vulnerability and pay remedies to any harmed parties. This includes the cost of notifying customers – now required by law in almost every state. The company can also suffer damage to its reputation and from the interruption to its business.

### ILLUSTRATIVE EXTRA-EXPENSE RISK SCENARIOS

- **Cloud security breach.** A marketing manager, impatient with his IT support personnel, buys cloud infrastructure for his department without informing anyone. He opts for the cheapest resource – one that offers only minimal security protection. A skilled cyber criminal hacks into the cloud provider, stealing names, addresses and bank account information for over 50,000 customers. Expenses include hiring an info-security firm to find and fix the breach, assisting with notification requirements, providing credit monitoring and a call center for impacted individuals, and creating an ID fraud policy for affected victims. The company also hires a PR firm to repair the damage to its reputation.
- **Personal failure to encrypt.** An employee buys a personal cloud storage plan from one of the popular storage services. She then moves company telecommunications credentials into the cloud without encrypting them. A cyber criminal executes a brute-force attack against her account, determining her username and password. The thief gains access to the unencrypted company credentials and sells them on the dark web, allowing multiple calls to foreign countries and causing telecom expenses to skyrocket.





# Minimize exposure to risk categories

Wherever we find technological breakthroughs, security risk is never far behind. However, through careful analysis of standard operating procedures, IT leaders can manage the threat landscape while allowing employees the room they need to accomplish their missions with the technologies that they are most comfortable with.

It is important to note that due diligence falls to designated technology leaders to evaluate mitigating measures, and not every action will be appropriate for each firm's unique needs. As executives continue to address the risks of Shadow IT within their companies, they can consider the following actions to help minimize their exposure to key risks:



## INTERNAL POLICIES AND PERSONNEL MANAGEMENT

## SOLUTIONS

- **Establish and enforce corporate policies and procedures.** Corporations can add policies to their employee handbooks that cover the most common types of Shadow IT usage. They can also take steps to educate employees on these policies and the consequences for violating them. Some Shadow IT techniques, like unreported cloud arrangements for company use, will apply more to managers, while others such as personal mobile and USB devices and individual cloud storage usage should target all employees. For personal smartphones and tablets, the policy should also address liability in the event a device is lost or stolen, and state whose responsibility it is to recover data if necessary. IT should also explain the privacy implications of such recovery operations.
- **Hire and train effective security administrators.** Check all references and certifications of all potential security employees. Encourage (or require) information security personnel to obtain industry security certifications such as CompTIA Security+, Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).
- **Educate end users.** Most successful cyber attacks occur as the result of the actions of unsuspecting users. As a first line of defense, IT should consider offering periodic training on common attack techniques and any new zero-day attacks that have developed since the last employee training sessions.



- **Vet all external developers' security practices.** Not all outsourced software development firms follow security practices. If internal programmers cannot fill the need for custom software, it's smart to buy from established companies with contract terms and conditions that hold them financially responsible for security, patches and upgrades.
- **Establish an approved vendor list.** Rather than discourage business managers from using external vendors for cloud or other services, companies should consider taking the initiative to vet external vendors themselves. Ensure that each is properly certified, qualified and in legal compliance. These steps will allow the creation of a company catalog of secure external IT service providers.
- **Establish data breach notification procedures before starting work with any vendor.** Include language in vendor contracts requiring the vendor to provide timely notification and collaboration to manage any data breach problem the vendor may have caused.



- **Perform comprehensive threat analysis.** Before CTOs can take any action to enhance their information security, they must first know what threats exist in their environments. If they don't have the automated tools or in-house talent to perform this analysis, they should consider outsourcing the task to an information security firm.
- **Establish company-secured cloud file sharing.** Administrators should consider creating their own cloud-based file-sharing alternatives to Box, Dropbox, iCloud and Google Drive. IT can assign security keys and credentials to employees for the file-sharing system, providing much-needed visibility to sensitive data movement.
- **Secure the shop floor.** All network-connected devices in a manufacturing operation are valid network nodes and must be secured just like servers and desktop computers.
- **Encrypt, encrypt, encrypt.** Encryption is the greatest defensive weapon companies have available in the war against cyber crime. This is particularly true for personal mobile devices in the workplace that might contain private, sensitive company data. Any sensitive data moved to cloud data sources should be encrypted before being moved. Encryption keys should never be placed in the same cloud as the data.
- **Inventory all technology assets.** Take inventory of all corporate-owned hardware, tag the hardware and make hardware traceable whenever possible. Creating a baseline of owned devices is important for detecting foreign devices that connect to company networks as Shadow IT nodes. Run periodic scans on all workstations to detect unauthorized software installations. Unauthorized equipment, software or applications should be removed. Keep this list updated as workers start and end their tenure with the company.
- **Require security software.** Some employees truly are more productive when they can use their own equipment. But their machines should be equipped with the same anti-virus and security software as other computers in the firm. Consider requiring that any personally owned devices have company-mandated security checks, complete with auditing features controlled by the IT department.
- **Acquire Shadow IT detection packages.** Many security vendors offer enterprise software packages to detect things like unauthorized cloud usage. Some of the more mature enterprise mobility management packages allow firms to control data on users' personal mobile devices and wipe them clean in the event of a loss or theft.
- **Require greater security for administrator accounts.** As the company grows, more people will be granted administrator rights with more authority and privileges. Because administrators have more power, they should have more stringent policies governing any network actions they perform.





Contract practices can impact technology errors and omissions risk. To help manage this risk, companies should evaluate the following customer contract provisions:

- **Limitation of liability.** This provision disclaims liability for certain types of damages – usually incidental, consequential or special damages. In the event of threatened or actual litigation, these provisions can become very useful.
- **Damage caps.** These provisions can be defined in terms of a specific dollar amount or an amount to be determined, depending on specific factors defined in the contract.
- **Disclaimer/Limitation of warranties.** This provision identifies the warranties provided, disclaims or limits those warranties not provided, and identifies the remedies available in the event the product or work does not comply with the warranties provided.
- **Integration.** This provision identifies the documents that comprise the parties' contract, and will also limit the parties' reliance on documents and information outside of the contract.
- **Contractual risk transfer and defense/indemnity provisions.** Provisions like these can shift risk to other parties, as appropriate.






# Insurance considerations for Shadow IT

Most corporate leaders agree that Shadow IT is both a blessing and a curse. They also agree that the trend will continue as long as employees and managers can get their technology needs met from sources other than their own corporate IT departments.

Shadow IT is everywhere, and the risks are difficult to see, much less manage. Hackers worldwide are coming up with new and creative ways to take advantage of the vulnerabilities Shadow IT creates.

Companies can investigate insurance options with their independent agent or broker. Consider the following:

		
Risk class	Illustrative risk scenarios	Relevant insurance coverage to evaluate with an agent or broker
<b>Bodily injury</b>	<ul style="list-style-type: none"> <li>• City social engineering</li> </ul>	<b>Products liability coverage</b> provides coverage for physical harm to a person arising out of a product manufactured, sold, handled, distributed or disposed of by a named insured.
<b>Technology errors and omissions</b>	<ul style="list-style-type: none"> <li>• Failure to test</li> <li>• Software not fit for intended use</li> <li>• Flawed code</li> </ul>	<b>Errors &amp; Omissions (E&amp;O) liability coverage</b> protects against damages that you must pay because of economic loss resulting from your products or your work, and caused by an error, omission or negligent act.
<b>Cyber risk</b>	<ul style="list-style-type: none"> <li>• Untrained team member</li> <li>• Trojan malware-infected thumb drive</li> <li>• Non-encryption violation</li> </ul>	<b>Information security coverage</b> provides coverage for critical cyber risks. Coverage options vary, but most include network and information security liability and communications and media liability.
<b>Extra expenses</b>	<ul style="list-style-type: none"> <li>• Cloud security breach</li> <li>• Personal failure to encrypt</li> </ul>	<b>First-party expense reimbursement coverage</b> options often include data restoration, business interruption, computer and funds transfer fraud, crisis management, and security breach notification expenses.

## Circumstances vary, and not all risks are insurable.

It is important to contact your independent insurance agent or broker to make sure that you get the right coverage and services for your company.

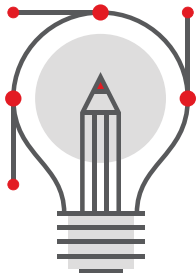


# How Travelers can help

Travelers has been insuring technology companies longer than most insurers, and we understand the unique risks they face. As you continue to work diligently to secure your company's IT practices, Travelers can help manage risks with the right insurance products.

From the rise of PCs, the Y2K scare, the internet economy and now the IoT, Travelers continues to evolve with coverage solutions that provide peace of mind to technology companies as they continue to innovate.

Shadow IT has the potential to bring business benefits to technology companies, as long as the risks are managed. For more information, contact your independent insurance agent who represents Travelers Technology or visit us on the web at [travelers.com/technology](http://travelers.com/technology).



Travelers continues to evolve with coverage solutions that provide peace of mind to technology companies as they continue to innovate.





## RESOURCES

---

- Earle, Nick, “Do You Know the Way to Ballylickey? Shadow IT and the CIO Dilemma”, Cisco, Aug 2015, accessed Dec 2015, <http://blogs.cisco.com/cloud/Shadow-it-and-the-cio-dilemma>
- Corbin, Kenneth, “How CIOs Can Reduce Shadow IT in Government”, CIO, Jun 2015, accessed Dec 2015, <http://www.cio.com/article/2929782/it-management/how-cios-can-reduce-shadow-it-in-government.html>
- “Hiring managers are desperately seeking tech workers with these skills”, Jan 2016, accessed Jul 2016, Monster.com, <http://www.monster.com/technology/a/most-difficult-tech-skills-to-find>
- Basani, Vijay, “Study Shows IT Departments are Understaffed”, EiQ Networks Blog, Aug 2015, accessed Jul 2016, <http://blog.eiqnetworks.com/blog/study-shows-it-departments-are-understaffed>
- “Understaffed and at Risk”, Ponemon Institute, Feb 2014, accessed Jul 2016, [http://www.hp.com/hpinfo/newsroom/press\\_kits/2014/RSAConference2014/Ponemon\\_IT\\_Security\\_Jobs\\_Report.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_IT_Security_Jobs_Report.pdf)
- “Strict Approval Processes Slow Down Tech Adoption”, eMarketer, Aug 2015, accessed Dec 2015, <http://www.emarketer.com/Article/Strict-Approval-Processes-Slow-Down-Tech-Adoption/1012883>
- Lewis, Bob, “12 Bad Habits that Slow IT to a Crawl”, Info World, Sep 2015, accessed Dec 2015, <http://www.infoworld.com/article/2982389/it-management/12-bad-habits-slow-it.html>
- Bradley, Tony, “Pros and Cons of Bringing Your Own Device to Work”, PC World, 2015, accessed Dec 2015, [http://www.pcmag.com/article/246760/pros\\_and\\_cons\\_of\\_byod\\_bring\\_your\\_own\\_device.html](http://www.pcmag.com/article/246760/pros_and_cons_of_byod_bring_your_own_device.html)
- Korolov, Maria, “Only 8 Percent of Companies Can Track Shadow IT”, CIO, Jan 2015, accessed Dec 2015, <http://www.cio.com/article/2868113/it-organization/only-8-percent-of-companies-can-track-shadow-it.html>
- Palmer, Danny, “hackers see cloud as a fruit bearing jackpot for cyber attacks”, Oct 2015, accessed Dec 2015, <http://www.computing.co.uk/ctg/news/2429256/hackers-see-cloud-as-a-fruit-bearing-jackpot-for-cyber-attacks>
- Allison, Diana, “Bring Shadow IT Out of the Dark, Gartner Tells Tech”, Enterprise Tech, Jun 2015, accessed Dec 2015, <http://www.enterprisetech.com/2015/06/17/bring-shadow-it-out-of-the-dark-gartner-tells-tech/>
- Nachenberg, Carey, “A Window into Mobile Device Security. Examining the Security Approaches Employed in Apple’s iOS and Google’s Android”, Symantec, 2011, accessed Dec 2015, [http://www.symantec.com/content/en/us/enterprise/white\\_papers/b-mobile-device-security\\_WP.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/white_papers/b-mobile-device-security_WP.en-us.pdf)
- “Bring your own device. Security and risk considerations for your mobile device program”, EY, Sep 2013, accessed Dec 2015, [http://www.ey.com/Publication/vwLUAssets/EY\\_-\\_Bring\\_your\\_own\\_device:\\_mobile\\_security\\_and\\_risk/\\$FILE/Bring\\_your\\_own\\_device.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf)
- Lipman, Becca, “Why senior executives are risk management’s worst enemy”, Wall Street & Technology, Jan 2014, accessed Dec 2015, <http://www.wallstreetandtech.com/risk-management/why-senior-executives-are-risk-managements-worst-enemy/d/d-id/1268661?>
- Ferrara, Joe, “Phishing Attacks Explode and Executives Are Taking the Bait”, SC Magazine, Aug 2013, accessed Dec 2015, <http://www.scmagazine.com/phishing-attacks-explode-and-executives-are-taking-the-bait/article/306453/>
- Cluley, Graham, “Danger USB! Could a Flash Drive’s Firmware Be Hiding Undetectable Malware?”, The State of Security, Aug 2014, accessed Dec 2015, <http://www.tripwire.com/state-of-security/security-data-protection/danger-usb/>
- “2015 Cost of Cyber Crime Study: United States”, Ponemon Institute, Oct 2015, accessed Jul 2016, <http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states>
- Lynch, Eric J, “How to Bring Shadow IT into the Light”, Rackspace, Jun 2014, accessed Dec 2015, [http://pages.rackspace.com/Global/FileLib/VMWare/150120\\_Bring\\_Shadow\\_IT\\_Into\\_Light\\_ANZ.pdf](http://pages.rackspace.com/Global/FileLib/VMWare/150120_Bring_Shadow_IT_Into_Light_ANZ.pdf)

# Risk expertise for the technology industry



Travelers has been insuring technology companies for more than 30 years. Hear directly from Travelers technology industry experts, using the links below.



**MITCH FOSTER II**  
**ON TELECOM:**  
[travl.rs/1cgWzik](https://travl.rs/1cgWzik)



**KIRSTIN SIMONSON**  
**ON INFORMATION TECHNOLOGY:**  
[travl.rs/1PL9YBL](https://travl.rs/1PL9YBL)



**PATTY NICHOLS**  
**ON MEDICAL TECHNOLOGY:**  
[travl.rs/1FVhMwf](https://travl.rs/1FVhMwf)



**JILL DUFFY**  
**ON GLOBAL RISKS:**  
[travl.rs/1FVhhIL](https://travl.rs/1FVhhIL)



**MIKE THOMA AND RONDA WESCOTT**  
**ON INSURING TECHNOLOGY COMPANIES:**  
[travl.rs/1F8WjZR](https://travl.rs/1F8WjZR)



**RYAN STROUTH AND MIKE DEHETRE**  
**ON EMERGING TECHNOLOGY:**  
[travl.rs/1BnJyKw](https://travl.rs/1BnJyKw)



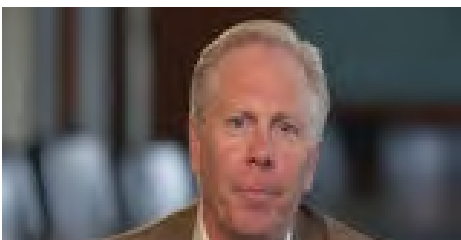
**CLAIRE KORNEGAY AND KIRSTIN SIMONSON**  
**ON CYBER RISKS:**  
[travl.rs/1J3jASH](https://travl.rs/1J3jASH)



**MITCH FOSTER II**  
**ON ELECTRONICS MANUFACTURING:**  
[travl.rs/1Fep5cv](https://travl.rs/1Fep5cv)



**EILEEN KAUFFMAN**  
**ON CLEAN TECHNOLOGY:**  
[travl.rs/1LGy5f8](https://travl.rs/1LGy5f8)



**MIKE THOMA**  
**ON LARGE TECHNOLOGY COMPANIES:**  
[travl.rs/224uxN5](https://travl.rs/224uxN5)



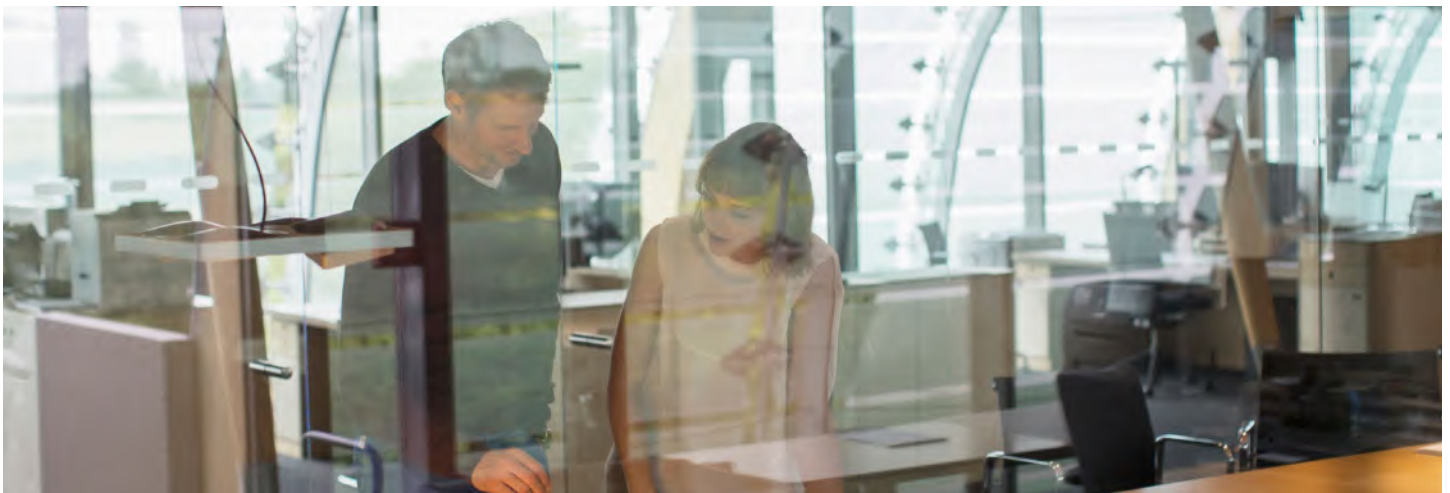
**LINSEY MCDONALD**  
**ON TECHNOLOGY RISK CONTROL:**  
[travl.rs/1RmABNd](https://travl.rs/1RmABNd)



**JERRY GALLIVAN**  
**ON TECHNOLOGY CLAIM:**  
[travl.rs/1OtUUCI](https://travl.rs/1OtUUCI)

“Right now, Shadow IT may be endangering your intellectual property and sensitive customer or employee data. Before you can take concrete steps to protect your technology business, you must first understand the nature and scope of this risk.”

**Mike Thoma**, *Practice Lead and Chief Underwriting Officer,*  
*Travelers Global Technology*



---

For more information, contact your independent insurance agent who represents Travelers, or visit us on the web at [travelers.com/technology](https://travelers.com/technology).

---



[travelers.com](https://travelers.com)

The Travelers Indemnity Company and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material is for informational purposes only. All statements herein are subject to the provisions, exclusions and conditions of the applicable policy. For an actual description of all coverages, terms and conditions, refer to the insurance policy. Coverages are subject to individual insureds meeting our underwriting qualifications and to state availability.

© 2019 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. BTCWH.0004 New 8-19