## TABLE OF CONTENTS

OVERVIEW ................................................................. 3  
KEY FINDINGS ........................................................... 4  
METHODOLOGY AND SCOPE ............................................ 5  
MAJOR RISKS AND MITIGATION STRATEGIES ....................... 6  
BUSINESS STRATEGY .................................................... 6  
MANAGEMENT AND GOVERNANCE ..................................... 9  
POLICY AND PROCEDURE ............................................... 11  
SECURITY MAINTENANCE ............................................... 12  
PHYSICAL SECURITY .................................................... 14  
TECHNICAL CONTROLS .................................................. 16  
CONCLUSION ............................................................... 19
The cyberattack surface and threat landscape are flourishing by the day. The amount of data handled by businesses is proliferating to astounding levels. And the size and management complexity of IT infrastructure is exponentially expanding as well. All of this adds up to organizations having to cover more ground from a security standpoint than ever before. Yet businesses often lack the in-house skills, resources, leadership-level support and general visibility to ensure every area of risk is adequately attended to.

As such, assessments of one’s risk profile help document areas of exposure and guide organizations to prioritize where they should apply the most attention (and dollars) so they can attain risk levels that owners, boards of directors and C-Level executives find acceptable. These assessments also help companies implement the appropriate controls, ensure a sufficient balance of functionality versus protection, and defend and respond to cybersecurity threats and incidents in an effective and efficient manner.

Over the past 16 months, Trustwave tasked a third-party firm to query IT professionals to answer questions about their organization’s susceptibility to risk. The questions covered the areas of business strategy, management/governance, policies/procedures, security maintenance, physical security and technical controls. We aggregated and compiled the 476 responses to bring you the 2014 State of Risk Report.

This report helps identify the most common points of deficiency across organizations, spanning geography and industry. It offers benchmarks by which IT and security professionals can compare their risk stance against their peers. The data also can be used to properly inform senior leadership about the largest threats they are facing and gaps that need filling. But arguably most important is that the report presents actionable best practices and technology suggestions that practitioners can use to manage, assess and address these areas of common weakness.
HERE ARE SOME KEY FINDINGS:

• 81% of businesses store and process financial data.

• 63% of businesses do not have a fully mature method to control and track sensitive data. 19% have none at all.

• 68% of businesses transfer sensitive data between locations; 58% of businesses use third parties to manage sensitive data, yet almost half (48%) do not have a third-party management program in place.

• 38% of IT professionals say their businesses do not have technical controls in place to allow employees to use their own devices (BYOD) securely; 33% do not have policy controls in place surrounding BYOD.

• 45% of businesses have board- or senior-level management who take only a partial role in security matters. 9% do not partake at all.

• 60% of businesses are fully aware of their legal responsibilities in safeguarding sensitive data, yet 21% of businesses never perform security awareness training, 23% never hold security planning meetings and 24% do not have employees that read and sign their businesses’ information security policy.

• 50% of businesses run internal vulnerability scans on critical systems (self-hosted) less frequently than every quarter. 60% run external vulnerability scans on critical systems (third-party hosted) less frequently than every quarter. Meanwhile, 18% never perform penetration tests.

• 58% of businesses do not have a fully mature patch management process in place, and 12% do not have a patch management process in place at all.

• 33% of businesses have not commissioned a risk assessment.

• 21% of businesses do not have incident response procedures in place.

• 20% of businesses do not have a process that enables the reporting of security incidents.
METHODOLOGY AND SCOPE

• During a 16-month period, from July 2013 to November 2014, Trustwave engaged a third-party firm to ask information technology professionals to complete a web-based survey querying them on IT and security risk maturity within their organizations.

• The 476 respondents were primarily based in the United States, United Kingdom and United Arab Emirates, although the total pool hailed from more than 50 countries.

• Respondents, who all had information technology or information security roles, included:
  • Technology Director or Manager (38%)
  • Network/System Administrator (15%)
  • IT Executive (CIO, CTO, or other) (13%)
  • Security Technology Director or Manager (10%)
  • Other (24%)

• Respondents were spread across a wide variety of industry sectors, primarily consisting of technology, financial services and business services. Three-quarters of respondents came from small- and medium-sized businesses up to 1,000 employees.
MAJOR RISKS AND MITIGATION STRATEGIES

BUSINESS STRATEGY

Data, from customer information to intellectual property, is the lifeblood of most businesses. Yet many organizations are unaware of the amount of confidential assets under their roof and where they are located. Knowing where your data lives and what you need to do to protect it is a big part of the battle to prevent breaches and make your company less vulnerable to theft.

476 IT PROFESSIONALS SURVEYED

| Store and Process Financial Data | 81% |
| Store and Process Payment Card Data | 47% |
| Use Batch Processing When Working and Interacting with Sensitive Data | 59% |
| Store and Process Intellectual Property Data | 71% |
| Work and Interact with Sensitive Data Online | 78% |

TIPS

Designate a specific person who will maintain up-to-date information on financial data regulations and legislation. Ensure policies and processes are in place to handle financial data appropriately.

Understand the full flow of payment card data. Only store what you absolutely need. Designate a specific person who will maintain up-to-date information on the Payment Card Industry Data Security Standard payment card requirements. Consider PCI compliance the ground floor for overall security.

Batch processing offers greater efficiency in processing sensitive data, but it opens up risk. Test all batch processes regularly to ensure everything is operating securely and correctly. Review all processes each time a major change is made.

Identify any intellectual property and ensure policies, procedures and technologies are in place to protect it.

Remember your web presence goes beyond your own website. Consider running a vulnerability management program that includes penetration testing, vulnerability and database scanning, application security settings checks, cloud security and risk assessments to help ensure the protection of sensitive data.
Access control and risk assessments should be performed regularly. These tests will give you visibility into high-risk areas in your organization’s operational policies and processes.

Ensure all of the appropriate contracts are in place before any B2B integration takes place. Service-level agreements (SLAs) help ensure that all parties understand their roles and responsibilities. Designate a trained and experienced person to lead these obligations.

Before allowing any third party to access or host your facilities, data and systems, you need to sign off on all appropriate contracts and agreements. These include non-disclosure agreements, service-level agreements and appropriate certifications. Also consider legal issues, depending on jurisdiction.

Third-party programs should be updated in line with compliance obligations, as well as changes in the risk landscape. Regularly review and manage the level of risk you are exposed to as a result of these relationships, and investigate any incidents related to these third parties.

Malware is the preferred vehicle by which external attackers steal sensitive information, such as credit cards and non-payment data, including intellectual property. IT pros require advanced solutions that can spot and block malware, zero-day vulnerabilities and advanced persistent and blended threats in real time. Companies that lack the necessary in-house skills, resources and budget to handle malware themselves can partner with a managed security services provider.
Maintain visibility by keeping logs of all devices as they are introduced and removed from your network.

Ensure that employees are aware of what is permitted to connect to your networks. Review policies regularly to ensure full visibility of what is connecting.

HAVE POLICY CONTROLS IN PLACE TO ALLOW EMPLOYEES TO USE THEIR OWN DEVICES (BYOD)

HAVE TECHNICAL CONTROLS IN PLACE TO ALLOW EMPLOYEES TO USE THEIR OWN DEVICES (BYOD)

SOLUTION SPOTLIGHT

NETWORK ACCESS CONTROL

Network Access Control enables granular control over network access and provides continuous monitoring of corporate-sanctioned and bring-your-own-device (BYOD) endpoints. This can help you prevent the spread of malware and other threats. Companies that lack the necessary in-house skills, resources and budget should consider partnering with a managed security services provider.

PERFORM REGULAR SECURITY AWARENESS TRAINING

Employees, if properly trained, can be be a valuable front-line defense for any size organization. Implement a regular awareness and training program covering both policy and procedures. Maintain a process to confirm staff members have attended all relevant training programs and can demonstrate a strong understanding of corporate policies and procedures. Don’t forget to ensure third parties are trained as well.

SOLUTION SPOTLIGHT

SECURITY EDUCATION

Security Awareness Educations provides employees with the tools they need to help protect data. Educated employees help strengthen the so-called weakest link and reduce the chances that your business will become a victim of today’s information security threats.
Never before has cybersecurity been so important to discuss in the boardroom. Management at all levels is becoming increasingly aware of the business impact – lost customers, tarnished reputation, compliance fines and litigation fees – that a breach can cause. Without input from these levels, security performance and appropriate resource allocation can suffer. In addition, communication breakdowns could occur, limiting the IT department’s ability to implement companywide plans. And even when management is fully engaged, organizations must ensure follow-through: that security measures, like incident response and training, are being established.

For board members to properly understand security and risk, and to enable them to make the right choices, you must provide them with easy-to-understand and accurate information.

Senior management must understand and engage with the risk and security issues that impact their operational areas. Ensure proper and clear communication among business departments and technical teams.

If employees at all levels of the business do not take an active role in security, there is a higher chance of your company’s assets being exposed.

**RISK CHECKLIST: CONNECT MANAGEMENT WITH SECURITY**

- Review your corporate governance frameworks annually, as well as at any major business change.
- Validate that corporate governance changes are approved by senior management.
- Ensure that risk management culture is endorsed from the top.
- Use clear and simple communication to encourage top-level buy-in.
Discussion of security issues is central to managing your organization’s risks and vulnerabilities. Your business is always evolving, adapting to markets and customers. Ensure the frequency of security planning meetings reflects the pace of change in your organization.

Operate a thorough risk management program, supervised by senior management. Perform comprehensive risk assessments at least once a year and more often where needed. Remember to consider control processes, as well as regulatory and compliance obligations.

Review your business continuity plan (BCP) at least quarterly and evaluate the process annually. Test everyone involved in the BCP on the process to ensure they are aware of their responsibilities. And regularly update your plan to reflect any changes in the organization.

Having processes in place and testing them regularly will help ensure the appropriate people have the right knowledge and skills to respond rapidly to unforeseen problems. Coordinate a regular meeting with all key people involved in the incident response process.

SOLUTION SPOTLIGHT

INCIDENT RESPONSE AND READINESS

When a breach happens, organizations that can determine the cause and respond quickly to mitigate damage and collect the necessary information to thoroughly investigate will save themselves costly expenses. Preparation also is key – businesses must be able to recognize indicators of compromise.

Natural or man-made disasters can strike at any time, disrupting or disabling your ability to process data, and interrupting or destroying your organization’s operations. Review and update your disaster recovery processes quarterly to ensure they keep pace with changes in your business. Ensure that key staff meets regularly to discuss.
Policies and procedures lay a critical security groundwork within organizations. These rules establish agreed-upon buy-in from all levels and departments of a business and help ensure that all employees understand their roles and responsibilities when it comes to preventing attacks, defending sensitive data and responding to incidents. All policies and procedures should be reviewed regularly to ensure they help businesses meet their goals.

Ensure a process is in place where employees and third parties can report events no matter how minor they appear - immediately and without fear of reprisal. Study previous incidents so you can learn from any past mistakes.

Legislation changes as technology matures and evolves. Stay up to date on these changes and adapt security policies to meet requirements. Review controls every quarter.

Make all staff aware of policies and procedures - which should be written in understandable language and free of jargon - as soon as they join the organization, and ask them to review every quarter.

RISK CHECKLIST:
ENSURE THESE AREAS ARE PART OF YOUR POLICIES AND PROCEDURES

- Organization and classification of information security
- Asset management
- Human resources
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Regulatory compliance
Without properly caring for the systems within a business, a simple change made to them can result in a successful breach. Organizations must be aware of all of the devices connected to their network that may introduce exposure or vulnerability. In addition, they must have processes in place to test these environments and fix any weaknesses that are discovered.

Internal vulnerability scans are key to keeping an organization’s infrastructure secure and protected. Vulnerability scans assist the IT and security departments in identifying business assets that are not being patched and appropriately secured.

Ensure all public networks and interfaces are included in your organization’s vulnerability management program. External vulnerability scans should be conducted quarterly. There are approved scanning vendors that can provide this service.

### RISK CHECKLIST:

**BUILD A VULNERABILITY MANAGEMENT AND SECURITY TESTING PROGRAM**

- ✔️ Update your vulnerability management and penetration testing programs with the latest security requirements.
- ✔️ Make sure your vulnerability management and penetration testing programs are part of your risk, change control, compliance and corporate governance initiatives.
- ✔️ Prioritize any vulnerability findings and communicate them to allow senior management to help assess the level of risk.
- ✔️ Ensure that the resources operating and developing your systems are not the same as the resources overseeing your vulnerability management and penetration testing programs.
- ✔️ Review the security model being used to secure your data, if you are using a third party to run your security management programs and to store your vulnerability database.
- ✔️ Confirm the vulnerability and associated risk is no longer present in your systems once you have mitigated a weakness.
Penetration tests are key to an organization’s security and risk program, allowing you to better understand the security and integrity of current infrastructure and business applications.

Patch management is often overlooked or implemented incorrectly. Audit your patch management program and prioritize which fixes are most important. At a minimum, patch Windows systems monthly. Patch systems in small groups to avoid pushing out a faulty fix, and review patch levels quarterly.

Change control is a process of managing change to an organization’s environment and assessing the potential impact on business. Review and police the change control process to ensure changes are not being made to systems without your knowledge. Form a review board to keep track of any changes and analyze how they might affect your organization’s processes.

SOLUTION SPOTLIGHT

VULNERABILITY MANAGEMENT

Vulnerability Management is a two-part process that includes conducting automated vulnerability scanning across all networks, applications and databases - augmented by in-depth penetration testing for businesses’ most critical assets. Businesses that lack the in-house skills and manpower to perform this themselves can partner with a managed security testing provider.
Organizations often have a misconception about the value of physical security and the assurance it provides. Physical security is key to protecting corporate assets and preventing security incidents. However, physical security controls are not just preventative, as they may also assist in post-security incident investigations and subsequent legal action or criminal proceedings.

Physical controls can help your organization ensure that critical infrastructure is accessible by approved personnel only, preventing unauthorized access until an attack can be detected and responded to by the appropriate security personnel.

RISK CHECKLIST:

1. **LOCK DOWN YOUR PHYSICAL ENTRYWAYS**
   - Regularly assess all physical security to ensure it meets business requirements.
   - Feed all physical requirements into risk management, change management and compliance regulatory programs.
   - Deploy secure IP-enabled surveillance that you can wirelessly connect to record images and video. Technologies, like card readers, also are important.
   - Perform regular social engineering tests, physically as well as digitally, to remind your staff of dangers.
   - Conduct background checks on third-party organizations and personnel.
   - Report any incidents to senior management.
Regularly review the personnel who need access to your operating locations. Impose the appropriate controls to ensure only the required access is granted. Monitor and record personnel who are entering sensitive areas.

Ensure only secure methods and protocols are used to transfer data between sites to minimize the risk of interception. Regularly review all permitted connections to ensure transfer processes keep pace with threats, regulations and technology.

Use strong encryption and store keys securely by minimizing the number of people who manage them. Regularly review encryption and key management processes.

### HAVE PHYSICAL CONTROLS IN PLACE TO LIMIT ACCESS TO SENSITIVE DATA AREAS (HIGH-SECURITY ZONES)

- **Fully**: 68%
- **Partially**: 27%
- **Not at all**: 5%

### TRANSFER SENSITIVE DATA BETWEEN LOCATIONS

- **Fully**: 68%

### ENCRYPT STORED SENSITIVE DATA

- **Fully**: 49%
- **Partially**: 31%
- **Not at all**: 20%
When it comes to monitoring security events and controlling access to sensitive data, technology plays a pivotal role. But as mentioned in the report, with any device or system that is connected to the network, security solutions also must be properly configured so that organizations can achieve the best results and gain full visibility into their infrastructure.

Firewalls and other security solutions are only fully functional if properly deployed, configured, monitored and managed.

**RISK CHECKLIST:**

**MAINTAIN SECURE NETWORK BOUNDARIES**

- Put the correct processes in place to ensure you have selected the appropriate network controls for your environment and have the resources to manage and maintain them.
- Implement network controls appropriately, checking and verifying their configuration.
- Include network controls in your change control, vulnerability and asset management programs.
- Perform regular reviews of the configurations of network control systems in your reporting and risk programs.
- Conduct vulnerability assessments and penetration tests on all network control systems upon implementation, and retest regularly.

Companies without configuration standards are likely to have systems with missing security settings on their networks. Develop a configuration management database to maintain and store all system configurations. Apply build standards, based on industry-recognized benchmarks, to ensure conformity across your infrastructure.
Identify confidential data and put in place appropriate policies and processes to ensure it is properly handled and protected.

Failing to review roles can result in employees gaining privileges far above their requirements. Implement role-based access controls and require business justification for access granted each role. Review roles and associated access levels at least quarterly.

**SOLUTION SPOTLIGHT**

**DATA LOSS PREVENTION**

Data Loss Prevention helps organizations discover, monitor and secure data at rest, in motion and in use to prevent exfiltration. Discovery of sensitive data allows security teams to focus their initiatives on specific users and systems, and then implement the appropriate measures to meet compliance requirements.

**SOLUTION SPOTLIGHT**

**THREAT MANAGEMENT**

SIEM is a software platform for organizations that want to detect threats, and manage risk and compliance requirements. It can include logging, correlation, dashboards and reporting, as well as ad-hoc analysis, forensic investigation capabilities, and powerful searching, filtering and visual analysis. Companies that lack the necessary in-house skills, resources and budget can partner with a managed security services provider for SIEM.
A centralized repository of system event data from across all business assets allows you to spot potential security problems and troubleshoot technical issues. Centrally store full details of all system events to establish full visibility. Implement automated alerting systems, monitoring data for indications of suspicious activity.

The use of technologies such as virtual desktops, proxy sessions and cloud computing can help ensure sensitive data is stored only on business-approved systems and not on untrusted devices. Be sure to minimize external access to your systems and networks, and regularly review permitted access levels.
With some declaring 2014 as the “Year of the Breach,” we may one day look back and also remember it for the year that information security once and for all left the territory of the technical and became a full-on business imperative. After all, how can such a move not be at least imminent? Considering the frequency of breaches and their staggering monetary and reputational costs, in addition to expanding compliance demands, any rational business leader would consider security practices fundamental to one’s ability to function and thrive, and a major component of one’s overall risk profile.

Yet considering the laundry list of high-profile brands that have sustained data-loss incidents this year, it remains clear that there is ample work to do across all size businesses. Companies continue to struggle to properly address deficient areas and prioritize where they should allocate resources. Compounding that plight is the fact that many organizations lack the necessary talent, skills and budget to properly address security in-house, in the first place. This is where delegating one’s security workload to a trusted and proven partner with security expertise and far-reaching threat intelligence could pay dividends in the long run.

This report serves as a valuable and meaningful starting point for IT professionals to understand where their organization is most likely to bear its largest security shortfalls and how to help rectify them. Aside from the technological guidance highlighted in the report, the suggestions for each of the various risk areas contained common themes. Let’s review:

COMMUNICATE: Every employee at a company plays a role in strengthening security and reducing risk. Many of those will need to be involved in discussions, but won’t necessarily feel comfortable. Breaking down the silos and simplifying the message is a key way to generate buy-in, from the corner office down to the rank-and-file.

IMPLEMENT PROCESSES: Any initiative that a company is undertaking is much more likely to have success if there is a plan and strategy in place. Following a blueprint for any security endeavor will net greater cohesiveness and efficiency.

TEAM UP: While it is important to designate certain individuals to take the lead on projects, teams can help build consensus and arrive at smarter decisions through debate and differing opinions.

REVIEW: A busy and evolving business is a good business. It’s also one that will have many moving parts. That is why it is critical to review processes and policies more often than you likely are doing now. Being more methodical and attentive in your review process will help you catch discrepancies sooner, thereby limiting the chances of being breached and allowing you to better handle a crisis if one arises.

Need help improving your state of risk? Visit www.trustwave.com to contact an advisor today.
Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than 2.7 million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective data protection, risk management and threat intelligence. Trustwave is a privately held company, headquartered in Chicago, with customers in 96 countries. 

For more information, visit https://www.trustwave.com.

©2014 Trustwave Holdings, Inc.