TURNING A BLIND EYE TO DATA SECURITY

Mending the Breakdown of Communication between CEOs & CIOs

Townsend SECURITY
Today the average data breach costs a company $5.5 million. At this price, data security is no longer an ‘IT problem’.

With the huge amount of sensitive data companies store and transfer today—from credit card numbers to names and home addresses—the risks associated with unprotected data are steadily and dramatically increasing. From hackers to employee mistakes the loss of sensitive data is considered such a critical issue that data protection is mandated not only by many industry segments but also by many state and governmental laws.

Despite these laws, massive data breaches continue to occur at an alarming rate that doesn’t appear to be slowing down, and possible data loss has become a business risk that many CEOs are unprepared to manage. Unlike financial discussions, a discussion on risks associated with IT security are often avoided or ignored completely due to the lack of communication between CEOs and CIOs in charge of securing company and customer data.

This eBook, designed for business executives, discusses the serious business risks associated with unprotected sensitive data and help provide you with tools and resources to begin the discussion about data security in your company.

Patrick Townsend
CEO, Townsend Security
INFORMATION SECURITY IS UP TO YOU /4

WHAT THE CEO NEEDS TO KNOW /8

5 COMMON MISCONCEPTIONS /11

STEPS TO TAKE /13

6 QUESTIONS TO ASK YOUR CIO /15

ABOUT THE AUTHORS /17
INFORMATION SECURITY IS UP TO YOU

When it comes to information security, many people within a business – from executives to end users – often assume that security is a technical issue that falls under the umbrella of duties performed by the IT department. These IT administrators manage network firewalls, clean up virus outbreaks, and manage the IT infrastructure. These tasks are often so far removed from the actual goings-on of the business, that few people in the company—including the CEO—truly understand the ever-evolving complexities of IT infrastructure and security.

With little understanding of these systems, databases and networks with sensitive data are left unsecured and at risk to hackers, network failures, and employee mistakes. Today, an average data breach costs a company $5.5 million. At this price, information security is not an IT problem. It’s so much more.
The Ponemon Institute surveyed 1,894 people in 12 countries in its 2012 *State of Global IT Security* study and found the main reasons why the appropriate steps are not being taken to improve information security are 1) insufficient resources, 2) it’s not a priority issue and 3) lack of clear leadership.

However, in most situations, good information security is achieved with easily accessible and simple solutions. In fact, in a 2012 study on data breaches, Verizon found that 96% of security attacks were not highly difficult, and were easily preventable. If security attacks are preventable, why are so many breaches occurring every year?

Today, businesses are constantly learning that their networks are wide open to attack, and they are learning this the hard way—through audit failures and data breaches. This is due not only to poor security practices. At a high level, contributing factors to the security problems we have involve people: politics, culture, and avoidance of difficult issues. The silos of policy, process and technology are also used to address different security requirements across different departments in extremely inefficient ways.

The result is enormous information systems complexities that the very people who are in charge are not able to manage. Worst of all, there is a distinct lack of oversight and accountability. We’re not managing information risks. Instead we are reactively putting out fires and trying to stay afloat. Imagine addressing critical areas such as finance or business operations in this way. Organizations that have taken this approach are no longer in business.
Any given business in any given industry has numerous regulatory, legal, and fiduciary responsibilities associated with information risk. Information security touches practically every aspect of a business. It is a business problem and it needs to be treated as such. The core information security principles we need have been around for several decades. Putting them into action is simply a matter of priorities. Regardless of how good your IT staff is and how responsible your users may be, it’s ultimately up to management to oversee the risks associated with their customers’ sensitive data. In the end, the management will be held responsible for theft or loss of that data.

A comprehensive information security program doesn’t require a complete retooling of the business. Nor does it need to be costly or complex. Security is as much about culture and process as it is policy and technology.

The security of your business hinges on the discussion you must have in order to make decisions, implement the proper controls, and build accountability at all levels of your organization.

Data Privacy for the Non-Technical Person

Learn about the most effective methods for protecting sensitive data from hackers and other data loss.

Click Here to Download Now
"YOU WOULDN’T USE A CHEAP BIKE LOCK TO PROTECT FORT KNOX"

Why WOULDN’T you use ENCRYPTION to protect your most VALUABLE ASSET?”

- PATRICK TOWNSEND
WHAT THE CEO NEEDS TO KNOW

In any organization, the CEO has many jobs. At the macro level, a CEO’s job is to instill a high level of confidence in his or her stakeholders, including customers, investors, employees, suppliers and partners. To accomplish this, a CEO must establish a level of trust with these stakeholders in order to inspire, encourage, and engage them to take part in the entity’s vision and pursuits. Ultimately, the organization uses its stakeholders’ trust—their confidence in the CEO and his or her team’s ability to execute—to grow and build its value.

Every business has inherent risks in its execution—such as hiring dependable employees and maintaining financial stability. In order for a CEO to instill the kind of confidence that increases a business’ value, he or she must be able to identify and address each of the risks in the business. Therefore, risk mitigation by nature becomes a core component of a CEO’s job.
Today, unprotected electronic data is a risk that CEOs cannot ignore.

In a pre-internet world, the risk of data loss was limited to a physical breach of an actual building. Security guards, fences, and access control systems were established to keep people away from sensitive information. However, as today’s world has become electronically connected at virtually every level, businesses need to focus not only on preventing access to data but also on protecting the data itself. This is where a comprehensive data protection strategy comes in to play.

Most CEOs are well aware that encryption methodologies were created for their CIOs to be able to protect data in their networks. However, encryption is such a new field that few CEOs understand all of the risks associated with unprotected data as well as evolving industry-based regulations which they must comply with.

CEOs may not know that even if their data is encrypted, without proper encryption key management, they are still at risk and do not comply with many industry regulations.

Without good key management practices, you are practically inviting hackers to break in to your system.

Without proper encryption key management, they are still at risk.
Most people who hear about data breaches in the news know that the costs encompass more than just those incurred by the owner of the data that has been compromised. The cost of a data breach falls directly upon the entity entrusted with the protection of the data. A breach can ultimately result in debilitating fines and resources lost during recovery. In many cases, losses are measured in millions of dollars per incident.

But the cost of a data breach doesn’t end with financial loss. If confidential customer information is stolen the effect on an organization's brand is often devastating. Blame often falls on business leaders, who were trusted to address and eliminate business risk. Many companies cannot recover from the market impact that occurs when customers and stakeholders no longer have confidence in the organization to protect sensitive data.

**THE ONLY VIABLE SOLUTION TO MITIGATE DATA SECURITY RISK**

is to ensure that you have an adequate **encryption and encryption key management** solution in place that meets all requirements for data protection and compliance regulations. Encryption key management is the most important part of the equation. You must not only protect the data, you must also protect the keys to the data. In the end, the inability to address this issue may cost you your company.
Many business executives are aware that hackers and data breaches pose a risk to their organizations, but they aren’t sure how much risk they really bear, or even how to assess the risk from a business point of view. Let’s look at some of the misconceptions executives have, and what steps they can take to minimize the risk.

Watch the video: Patrick Townsend, CEO & Founder of Townsend Security, discusses why unprotected data is a business problem.
5 Misconceptions About Data Security Risk

1. If we have a breach, we’ll just pay the fine.
   In many cases there will be fines for a data breach, but it is only a small part of the total cost. The cost of a breach also typically includes a forensics investigation, credit monitoring for customers, lost sales due to brand damage, and litigation costs.

2. We’ve never had a problem, so things are probably OK.
   This type of thinking is not a form of risk assessment. Since data breaches often take months to discover, you may not know that a breach has already occurred. Wishful thinking won’t help you prevent a breach.

3. My software vendors and consultants say they have everything under control.
   Today, many software vendors have not moved quickly enough to add encryption to their core products. It is not wise to rely on vague statements about data security from vendors and consultants.

4. My IT staff says we’ve done everything we can.
   IT departments may not have the resources or management directives they need to assess and address data security issues. Meeting management’s goals and objectives within a set of operational and budgetary constraints is not the same as meeting security best practices.

5. We are encrypting our data, we are doing everything we should.
   If you are encrypting your sensitive data, you’ve already made a good step forward. Do you know how and where your encryption keys are stored? Only good key management will truly protect your data.
Steps to Take to Reduce Security Risk

1 Talk About It
Discuss the importance of data security with all members of the organization’s leadership team. Then talk to your IT department. Data security is an ongoing process that involves every member of the organization, and will extend beyond your organization’s boundaries to vendors and service providers. Responsibility for data security belongs to everyone.

2 Assess Your Current Data Security Posture
If you have not had an external audit and assessment of your organization’s data security practices by a qualified security professional, now is the time to start. First, perform a data security assessment with an in-house consultant, security audit firm, or platform vendor to evaluate your current security posture. Find the location of all sensitive data. Lastly, evaluate the security of your backup tapes. The right security assessor will help you identify the most urgent problems, and help you prioritize your efforts. This process can also help you overcome any internal resistance to addressing the problem.

3 Invest in Encryption and Key Management
When you have located sensitive data that is not encrypted, start a project to encrypt it now. Don’t forget to invest in the necessary encryption key management devices to protect the encryption keys. If your risk assessment warrants, provide budgetary exceptions to address the problem. Invest where you need to, as soon as you can. When choosing an encryption and key management solution, you should also ask: Is our encryption industry standard and NIST certified, is our key management FIPS 140-2 validated, is our key management device an external hardware security module (HSM), and are we using dual control and separation of duties to reduce points of failure?

White Paper: AES Encryption & Related Concepts
What is Advanced Encryption Standard (AES) and why do you need good key management?
Click Here to Download Now
Strengthen your technology acquisition processes

Every organization relies on off-the-shelf software solutions to manage and run their business operations. If your core applications do not provide encryption and key management to protect data, put your vendors on notice that they must address this issue immediately, and ask for updates. All new technology acquisitions should incorporate data security requirements into the RFP process. Your organization will live with technology acquisition decisions for many years, and you don’t want to live with the threat of a data breach until you replace your solutions.

Create ongoing review processes and procedural controls

Performing one security assessment or passing one compliance audit will not provide the focus and attention needed to protect you from a data breach over time. You must conduct routine vulnerability scans, create new processes, and review points within the organization to ensure that you continue to monitor your security stance. Use good procedural controls to minimize the chances of fraud. Implement Dual Control and Separation of Duties to achieve a defensible data security stance. Your software vendors will need to provide systems that can support these goals.

10 questions to ask your KEY MANAGEMENT vendor

1. Is your key manager FIPS 140-2 certified? What is the certificate number?
2. Would you describe the encryption key payload as simple or complex? (It should be simple)
3. Is there a common key retrieval application interface on all platforms? What are the differences?
4. What platforms do you support for key retrieval? (Note any gaps in platform coverage)
5. Do you provide working sample code for the platforms I need? (Windows, Linux, UNIX, IBM i, IBM z)
6. Do you supply binary libraries for all Enterprise servers?
7. Do you have a Java key retrieval class and examples? Is it standard Java or JNI?
8. Do you charge separate license fees for each client operating system?
9. Do you require that we purchase consulting services from you? Why?
10. If I am an independent software vendor (ISV), can you brand and certify the solution for us?
You know you need to discuss data security with your Chief Information Officer. Are you armed with the right questions to ask? If you need a place to start, ask your IT leaders these six questions.

1. Are we electronically storing or transferring personally identifiable information (PII) such as names, home addresses, passwords, credit card information, social security numbers, or protected health information (PHI)?
   Your CISO should also be able to tell you the location of the data whether it is stored in-house, in a hosted environment, or in the cloud.

2. Are we encrypting our sensitive data?
   Industry regulations and many state laws mandate that you protect this data. You will fail a security audit if this data is unprotected.
6 QUESTIONS TO ASK YOUR CIO

3. Is that data encrypted using AES 128-bit encryption?
   AES is a standard set by the National Institute of Standards and Technology (NIST). You're company should only be using NIST certified AES encryption.

4. Are we protecting our encryption keys with a hardened hardware security module (HSM)? Where are the keys stored?
   Encryption keys should never be stored on the same device as the encrypted data.

5. Is the HSM device we use FIPS 140-2 certified?
   The Federal Information Processing Standard (FIPS) is a standard set by NIST for hardware and software modules used in cryptography. This certification is critical to meeting data security compliance requirements.

6. Are the keys being handled using dual control and separation of duties?
   These are two important key management best practices that prevent any one person from having total control over a key.

Podcast: Key Management Best Practices – What New PCI Regulations Say

What does meeting PCI DSS v2.0 mean for your company?
Learn more about:

- Current best practices
- What PCI has to say about integrated key management
- Dual control, separation of duties, and split knowledge

Click Here to Listen Now
### ABOUT THE AUTHORS

**Kevin Beaver, CISSP**  
Kevin Beaver is an information security consultant, expert witness, and professional speaker with Atlanta-based Principle Logic, LLC. With over 23 years of experience in the industry, Kevin specializes in performing independent security assessments revolving around information risk management. He has authored and co-authored ten books on information security including *The Practical Guide to HIPAA Privacy and Security Compliance* and *Hacking For Dummies*. In addition, he is the creator of the Security On Wheels information security audio books and blog, providing security learning for IT professionals on the go. Kevin can be reached at [www.principlelogic.com](http://www.principlelogic.com) and you can follow him in on Twitter at @kevinbeaver and connect to him on LinkedIn at [www.linkedin.com/in/kevinbeaver](http://www.linkedin.com/in/kevinbeaver).

**Todd Ostrander**  
Todd Ostrander is a professional with over 25 years of F1000, mid-market and emerging market startup experience. Throughout his career, he has been at the forefront of groundbreaking changes that create new markets and opportunities. While he has a broad range of skills from finance to procurement, strategic marketing and product strategy, his core functional expertise is in exploiting existing markets as well as identifying and creating new market opportunities with specific focus on go-to-market, intellectual property, and capitalization strategies. Within the technology industry, he has specific expertise in workflow management, Software as a Service (SaaS), wireless, digital marketing, and mobility.

**Patrick Townsend, Founder & CEO of Townsend Security**  
Patrick Townsend has been in the data security industry for more than 25 years and brings both a deep well of knowledge and a unique perspective to the subject. He speaks regularly on data protection and encryption key management topics. He has produced a series of educational videos available on YouTube, records podcasts on data privacy, and is a regular contributor to the company's blog, [web.townsendsecurity.com](http://web.townsendsecurity.com).