

Why End-to-End Data Protection Has Become a Business Reality

An Osterman Research Executive Brief

Published February 2011



Osterman Research, Inc.

P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

OVERVIEW

In February 2011, an individual pled guilty in court to hacking into various World Pay accounts and stealing \$10 millionⁱ. The email addresses of more than 1,300 individuals in Brisbane, Queensland were mistakenly included in an email to subscribers of the government's CityCycle programⁱⁱ. Personal information about a number of Xavier University students was stolen and a 32-year old man was charged with attempting to extort the university in exchange for not disclosing the informationⁱⁱⁱ. Each week more than 12,000 laptops are lost or stolen in US airports alone and 97% are never recovered^{iv}.

Osterman Research conducted a study of mid-sized and large organizations in 2010 that found that during the previous 12 months, 23% of organizations had sensitive or confidential information leaked – accidentally or maliciously – through email^v. Further, 9% of organizations experienced such a data leak through a social networking or Web 2.0 application, while 5% had information leaked through an instant messaging system. A more recent Osterman Research survey, conducted during January 2011, found that 21% of respondents believe there will possibly or probably be a major data breach in their own organizations during 2011^{vi}. Lost laptops accounted for 49% of the data breach incidents between 2005 and 2009^{vii}.

KEY TAKEAWAYS

Data loss is a real concern. While most incidences are inadvertent – sending a document containing sensitive information through email in clear text, storing intellectual property on an unprotected USB drive or smartphone, or losing a laptop while on a business trip – they represent a major problem for organizations on a number of levels. Data loss can result in brand damage, customer churn, loss of competitiveness and require expensive remediation efforts.

The bottom line is that data protection is no longer a nice to have: it is a business necessity that must be given high priority alongside organizations' other security initiatives.

ABOUT THIS ANALYST BRIEF

This brief offers an overview of the data protection problem and what steps organizations should take to address it. We also provide an overview of the data protection capabilities offered by Trend Micro, the sponsor of this document.

The Compounding Problem of Data Protection

THE NUMBER OF VENUES FOR DATA LOSS IS INCREASING

Employees generate valuable corporate data when they create presentations, financial reports, personnel records, press releases, engineering drawings, emails, purchase orders, contracts and other information. This information can contain intellectual property, confidential information or time-sensitive data. Over time, even small organizations generate enormous quantities of this type of sensitive content.

A critical problem facing organizations is how to manage the growing flood of data given the numerous threat vectors from which this information can be leaked. For example:

- Data is sent by and stored on endpoint devices like desktops, laptops, tablet PCs and smartphones.
- It is stored and transported on removable media like USB sticks and external hard drives.
- It is sent through messaging and collaboration systems like corporate email systems, personal Webmail, instant messaging clients and collaboration tools.
- Sensitive content can also be transmitted via the growing number of Web tools and Web 2.0 applications, such as Twitter, Skype or peer-to-peer file-sharing tools.
- Compounding the problem is the growing quantity of content being stored in the cloud that poses unique privacy and security challenges in these typically multi-tenant environments.

THE NETWORK IS BEING DEPERIMETERIZED

The problem of data loss is being made dramatically worse by the disintegration of the previously well-defined corporate perimeter. Back in the “old days” of corporate networks, there was a clear distinction between a) the IT-deployed infrastructure consisting of email systems and other IT-sanctioned tools and b) consumer systems like instant messaging clients and Webmail. Today, however, the growing use of platforms in the workplace that began as consumer-focused tools – things like personal Webmail, Twitter, personal smartphones and the like – have more or less evaporated the network perimeter. An employee-owned iPad or smartphone is as likely to store sensitive corporate data as it is to store an employee’s vacation photos and music downloads.

It is important to note that the reason for the deperimeterization of the corporate network is most often not some sort of subterfuge by employees. On the contrary, many employers require their employees to be reachable on personal mobile devices, or they encourage employees to work from home using their own computers. Many employees use personal Webmail systems to continue working when the corporate email system goes down. The vast majority of employees that work in an office check their work-related email from home after hours – often using their own devices.

THERE ARE MORE DATA PRIVACY LAWS

Further adding to the problem is that a growing number of countries around the world are increasing the penalties associated with data leaks. In the United States, 46 of the 50 US states now have statutes on the books that require owners of sensitive information to be notified if this information is leaked, either inadvertently, maliciously or through some sort of external attack. Canada has the Personal Information Protection and Electronic Documents Act, Europe the Data Protection Directive, in the UK the Data Protection Act, the Personal Information Protection Law in Japan and many other countries in Asia and South America have laws on the books. We can expect more – and increasingly more stringent – statutes during the next few years as the amount of sensitive information in transit and at rest grows at a rapid pace, and as the consequences of data breaches become more expensive.

The penalties for data leaks are numerous and serious. Violations of data breach notification laws require expensive remediation efforts, and result in damage to an organization’s brand, a loss of goodwill and reputation, and lawsuits. However, there can be even more serious

consequences of data breaches, such as the loss of competitiveness resulting from intellectual property loss like trade secrets or patent applications, leaks of internal discussions about corporate mergers or acquisitions, or the exposure of marketing and sales plans to competitors.

Keys to Effective Data Protection

Because of the very serious consequences of data leaks – and the relatively high probability that every organization will at some point experience a serious loss of sensitive or confidential data – there are three critical steps that every organization should undertake:

- **Use layered protection at every point where data loss can occur**
It is vital to protect all sensitive data both in transit and at rest. This means that sensitive information sent via email, an instant messaging system or a Web 2.0 application must be protected when it is sent internally and particularly when it is sent outside of the organization. Further, data stored on file servers, SharePoint repositories, public or private cloud environments, email servers, employee desktops or removable media, for example, must also be protected from both accidental and malicious data leaks. This means protecting data on every device that has access to the corporate network, as well as every port through which data can be sent.
- **Minimize the complexity of data protection**
Protecting against data loss can easily become a very complex undertaking if the right capabilities are not deployed, resulting in higher administrative costs and a higher likelihood of missing something that results in loss of sensitive data. Consequently, any data protection system must ensure that authorized users have access to the data they need, without causing disruption to business processes. Data protection must be centralized in order to make it as painless as possible to manage for both the IT and security functions within a company. Further, it is important to leverage key data protection components in existing security infrastructure to minimize cost, complexity and risk to an organization. This approach also reduces administrative workload to the greatest extent possible.

Another key element in simplifying data protection is to allow flexible deployment models that can adapt to changes in corporate requirements over time. This means that data protection will ideally take place for on-premise and cloud-based systems, as well as hybrid combinations of these delivery models.

- **Maximize protection while minimizing cost**
Finally, it is critical to maintain as secure a data protection system as possible – given risk tolerance – while being sensitive to minimizing capital cost outlays. Because IT departments have a growing set of capabilities to manage – and because many of them have experienced significant cuts in their budgets over the past couple of years – data protection should not impose an undue cost burden on IT.

Thoughts on Trend Micro's Data Protection Direction

In the interest of full disclosure, it is important to note that Osterman Research is an independent analyst firm that works with a variety of vendors in the data protection space. Further, we believe that there are a number of solid and reliable vendors serving this market. That said, we are impressed by Trend Micro's data protection offerings and roadmap for four important reasons:

- **Focused on minimizing the complexity of deploying data protection**

Trend Micro offers a broad range of core data protection capabilities that include Data Loss Prevention (DLP), Encryption and Device Control. These are offered as standalone solutions or as add-on modules that are tightly integrated into existing Trend Micro solutions, such as messaging security and endpoint protection. Extended data protection elements include File Integrity Monitoring and Web Site Protection leveraging the Deep Security and Vulnerability Management Services product lines. Taken together, these capabilities extend data protection across physical, virtual and cloud-based infrastructure.

The breadth of capabilities offered by Trend Micro enables the company to be a "one-stop-shop" in the context of data protection, allowing an entire suite of data protection products and services to be procured from a single vendor. This simplifies the procurement, deployment and management process, largely because there is but one vendor to contact if something goes awry. Further, the interaction between potentially incompatible solutions from multiple vendors is eliminated by using a single vendor for all data protection capabilities.

- **Designed to reduce total cost of ownership**

The availability of a wide variety of data protection capabilities from a single vendor yields tremendous operational efficiencies, driving down the total cost of ownership. Companies have also realized lower per-seat prices for their data protection purchases because more is being purchased from the same vendor. Overall, this results in important cost savings during the evaluation and procurement process, as well as over the entire lifecycle of the data protection infrastructure.

The resulting consistency in the look and feel of the various data protection systems can result in more efficient use of IT staff time, resulting in reduced IT labor costs. Pre-defined policies included in the offerings can speed the enablement of data protection capabilities and further reduce the total cost of ownership.

Also, it is important to note that many of Trend Micro's offerings already have DLP and device control capabilities built-in, allowing data protection capabilities to be turned on within existing products rather than requiring deployment of new solutions. Turning on the data protection feature in existing products can result in an 80-90% reduction in cost when compared to purchasing new systems.

- **Emphasizes the cloud delivery model**

Trend Micro – in its effort to help customers secure their journey to the cloud – continues aggressively to add cloud-based capabilities across its data protection portfolio. For

example, SecureCloud delivers key management and encryption solutions for public and private cloud environments and SafeSync offers data backup capabilities.

- **Overall vision**

A key element of Trend Micro's data protection strategy is its vision for protecting every potential point of data loss – endpoint to cloud - as well as providing centralized threat intelligence and policy management across the entire ecosystem. The company also offers Data Protection Project Consulting and Technical Account Management Services designed to accelerate time to protection and maximize the return on security investments.

SUMMARY

While Trend Micro does not currently provide a solution for every conceivable permutation of platform, application or devices currently in use; and while its Enterprise Security Manager is not yet as complete as it will be several months from now, the company's product and service set for data protection is among the most complete among leading security vendors. The company should be on any company's very short list of vendors that should be considered for data protection.

© 2011 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

ⁱ Source: DataBreaches.net

ⁱⁱ Source: Brisbane Times, February 4, 2011

ⁱⁱⁱ Source: *The (Cincinnati) Enquirer*, January 28, 2011

^{iv} Source: FBI <http://www.zdnet.com/blog/gadgetreviews/how-to-keep-your-laptop-from-being-stolen/1766> & Ponemon Institute "Airport Insecurity" report

^v Source: *Messaging and Web Security Market Trends, 2010-2013*, Osterman Research, Inc.

^{vi} Source: *Predictions for 2011*, Osterman Research, Inc.

^{vii} Source: *The Leaking Vault*, Suzanne Widup, published by the Digital Forensics Association, July 2010