



Guide to the ROI of Encryption

Data security from Check Point can cut
the cost of data exposure due to lost devices
by 90 percent

Contents

Executive summary	3
Gauging financial risks of information loss	4
Replacement costs	4
Recovery costs	4
Impact costs	5
Image costs	6
Typical costs and ROI with encryption	6
Total cost of ownership	7
Learn more	8

Executive summary

Encryption is a cyber security technology used to protect the confidentiality, integrity, and availability of information stored on or transmitted between computers. Encryption solutions from Check Point automatically obscure digital files and make them unreadable to unauthorized users. The software allows authorized users to automatically decrypt files for use with appropriate applications. The use of these solutions is transparent to users and provides a vital infrastructure service similar to electricity or gas.

The worth of encryption is a significant issue for the modern enterprise. In the early days of computing, digital resources were under an organization's strict control. The Internet did not exist yet and the transfer of digital files to computers outside an organization's sphere of control did not occur. Today, digital information can go anywhere easily. Previously, most cyber-security precautions have focused on preventing hackers and criminals from accessing sensitive computing resources via the network perimeter or endpoints. Now enterprises must also address the risk of losing portable computing devices that contains sensitive data.

Surveys indicate that up to 60 percent of information theft results from lost or stolen equipment. Every laptop, PC, personal digital assistant (PDA), portable music player, flash memory stick, external hard drive, smartphone, or any other mobile device that can store data is a potential weak point. It is impossible to always control who has possession of or transfers confidential files onto mobile devices. But, access to that information can always be controlled — with encryption.

This white paper from Check Point Software Technologies is about the economics of encryption. It assesses financial risks to information loss if an organization does not use encryption and how those losses can be reduced by using encryption. By using Check Point encryption solutions, organizations can cut the annual costs of data exposure resulting from the loss or theft of computing equipment by 90 percent or more.

Also read: Guide to the TCO of Encryption

Check Point presents a companion white paper on encryption economics titled, Guide to the Total Cost of Ownership of Encryption. It presents an analytical model to calculate the total cost of ownership (TCO) by specifying encryption-related operational events, frequency of those events, and the labor cost of those events. The model compares three-year costs for the Check Point Endpoint Security Full Disk Encryption data encryption product with two major competitors. Real-world variables show TCO of Check Point Endpoint Security Full Disk Encryption is dramatically lower — even if both competitors gave away their products with no license fees.

“Encryption is an essential tool for protecting data confidentiality and integrity.”

JON OLTSIK
Senior Analyst
Enterprise Strategy Group, Inc.

Gauging financial risks of information loss

There are four categories of potential costs incurred by organizations when computing equipment, with corporate information, is lost or stolen. These costs include replacement, recovery, impact, and brand image. Some of these costs are straightforward, such as the price of a computer or software. Others may vary by industry, pertinent regulations, and associated penalties, and other competitive market conditions. The following content describes these variables and how they may be affected in scenarios with and without encryption. Organizations may adjust these variables as they uniquely affect their business operations in projecting their own annual cost of risks of information loss.

Replacement costs

This category pertains to the physical replacement costs of lost or stolen computing equipment.

Hardware. The lost or stolen hardware may consist of one element, such as a laptop computer or smartphone. A common but increasingly dangerous scenario is when an employee or contractor forgets a briefcase in a cab or at some other location and consequently loses multiple company-owned devices. According to a survey by Check Point, travelers left 85,000 cell phones and 21,000 handheld computers in Chicago taxis during a six-month period in 2005.

Software. The replacement cost includes licenses to replace the operating system, word processing, spreadsheet, presentation, communication, security, utility, and any other pertinent business software.

Effect of encryption. Encryption does not reduce direct replacement costs of lost or stolen hardware or software.

Recovery costs

Recovery pertains mostly to the costs of labor required to deal with the administrative requirements of lost or stolen equipment and data. In some cases, people may be unable to perform work until equipment is replaced. The critical question for assessing exposure during the recovery process is, “Do we know what information is on the lost system?”

Police report. A corporate representative will need to gather and provide pertinent information to the appropriate police agency, including description of the incident, suspects, name and personal information about the person from whom the device(s) was/were lost or stolen, description of each device, serial numbers, software titles, estimated value, and any other information relevant to the incident. Some jurisdictions may require filing reports with multiple police agencies.

Insurance claims. The insurance claim process entails many of the same items as a police report. An organization may also be required to produce receipts for proof of purchase, which requires research by the accounting department.

Data recovery effort. The IT department will be required to configure a new device or devices to replace the lost or stolen gear. In addition to installation and configuration of software, the device will require restoration of the most recent

data backup. Recovery of old data may require digital or even physical retrieval of backup media from off-site storage. Recovery of data that was not backed up requires participation of other employees who may have copies.

User downtime. The person from whom the equipment was lost or stolen may be unable to perform some elements of work until the gear is replaced. The effect could be substantial if the stoppage of workflow affects sales or other revenue-driven activity.

Assessment of exposure. The corporate security team will need to assess the effect of exposure due to the potential release of sensitive corporate information. The effect will grow if the loss or theft includes personally identifiable information of customers—especially if it is subject to regulation and personal privacy laws. Assessment is the big ticket item under “recovery” because it entails manually examining backed up data files to determine what data was at risk. Assessment includes examination of email and attachments.

Effect of encryption. Encryption eliminates most of the requirement for assessment because encrypted data cannot be accessed by unauthorized people, so the loss only pertains to the lost equipment—not a company’s brand or intellectual property.

Impact costs

Impact costs pertain largely to compliance with regulations and laws about personally identifiable information that may have been exposed by lost or stolen equipment or breach of a network-attached device containing that information.

Regulatory compliance. Many government regulations and laws require companies holding personally identifiable information about customers or individuals to provide safeguards for this type of data. Examples include the Gramm-Leach-Bliley Act (GLBA) for the financial services industry and the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry. Failure to comply can result in civil and possibly criminal penalties, including fines and imprisonment.

Notifications. The United States Congress is set to pass a comprehensive national data breach notification bill, which would require companies that suffer data breaches of personally identifiable information to notify affected customers about the incident. Meanwhile, security breach legislation has been introduced in at least 35 states and adopted in at least 22. Individual notification of incidents, even if exposed data is not actually exploited, is costly and time consuming.

Account changes. Exposure of personally identifiable information can require a company to transfer customers to new accounts, which can trigger large administrative charges for incidents involving thousands of customers.

Credit checks. A company responsible for a breach of personally identifiable information may have to pay for personal credit checks and thwart identity theft with ongoing monitoring of credit for customers affected by the disclosure of data.

Customer support. A data breach can trigger extensive new demands on customer support staff responding to phone calls, email, and letters about the incident.

“The top-level encryption of the Check Point solution gives us the confidence that we are compliant and no matter what happens, our data is completely secure.”

GRANT ROBERTSON
IT Manager
H&R Block Australia

Market leader

Gartner ranked
Check Point as
a leader in its
MAGIC QUADRANT
for Mobile Data
Protection.

Gartner Research
Research Note, August 2006

Competitive advantage. News of lost, stolen, or breached customer data may translate into success for the competition. It gives them the ammunition they need to tarnish a company's reputation, and could result in a customer exodus—to them.

Security of employees/customers. Exposure of personally identifiable information can reveal home addresses of employees and customers, which could lead to personal harassment or possible physical harm. Obviously, lawsuits are one potential fallout due to data loss.

Effects of encryption. Encryption eliminates all effects of information loss because it prevents unauthorized people from accessing that data. Many laws requiring notification for breach of personally identifiable information exempt an affected company from notification if the lost or stolen data was encrypted.

Image costs

The value of image is "priceless." It is difficult to precisely gauge how customers and the public will react to news that a company's data was lost or stolen. A company's reputation may suffer in the wake of a data breach. In some cases, market capitalization of a public company has declined as investors sell its stock after hearing news of a data breach. Also, class-action lawsuits and regulatory fines have resulted from the same news.

A company that suffers lost or stolen data may encounter difficulty retaining existing customers and attracting new ones. For example, a large U.S. bank has said that the loss of one unencrypted laptop resulted in a loss of \$6.1 million. Whether the loss is thousands, tens of thousands, hundreds of thousands, or millions of dollars per incident, each dollar of loss can be prevented by using encryption.

Typical costs and ROI with encryption

The financial risks of data exposure resulting from lost or stolen computing devices are real but can be limited by using encryption. The technology prevents unauthorized access to encrypted data. The table below summarizes typical recurring annual costs in two scenarios: "unprotected" an organization that does not use encryption, and "protected" reflects the effect of an organization that uses encryption.

The numbers in the table are typical for mid-to-large-size organizations, but may vary depending upon business sector, applicable laws and penalties for information exposure, and other factors. On average, use of Check Point Endpoint Security Full Disk Encryption can eliminate 90 percent or more of the annual cost of risk caused by unintended exposure of corporate or personally identifiable data on lost or stolen devices.

Total cost of ownership

The other side of ROI is the total cost of ownership (TCO) for encryption. One element of TCO is how fast an organization can eliminate the recurring cost of the risks detailed above. The longer it takes to deploy encryption, the more an organization is likely to pay for the cost of risks in an unprotected environment. Deployment time for encryption varies depending upon the solution chosen by an

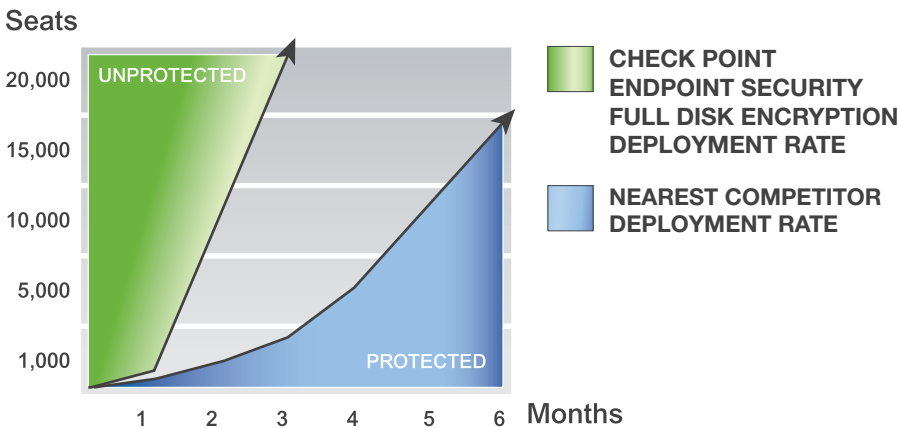
**TYPICAL RECURRING COST OF EXPOSURE—
NO ENCRYPTION VS. ENCRYPTION**

Cost element	Typical cost range (per incident)	Unprotected scenario	Protected scenario
Replacement — Lose equipment?	\$1,000 – \$3,000	\$1,500	\$1,500
Recovery — Know what information is on the lost system?	\$2,000 – \$10,000	\$6,000	\$1,000
Effect — Know what laws are applicable?	\$15,000 – \$10,000,000	\$22,500	\$0
Image — Know how customers and the public will react?	“Priceless”	High \$ Impact	Low \$ Impact
Average annual cost per loss incident	\$6,000 – \$3.3M +	\$30,000	\$2,500
Annual exposure: (assuming 3% annual loss of PCs on 1,000-seat installed base)	30 incidents	\$900,000	\$75,000

organization. Typical deployments for a large organization of tens of thousands of seats can require six months or more. Check Point Full Disk Encryption deploys much faster than competing products, based on the experience of enterprises replacing those products with Check Point Full Disk Encryption on hundreds of thousands of seats throughout the world.

The graph below compares the deployment rate for a 20,000 seat installation of encryption with Check Point Full Disk Encryption versus the deployment rate of the nearest competitor. With Check Point Full Disk Encryption, the job is done within three months while the competing product will require more than twice as much time.

An organization can calculate the economic value of superior deployment capability of Check Point Full Disk Encryption by leveraging data in the table on page 6. In that scenario, the annual recurring cost of risks is \$900,000 per each 1,000 seats in an organization. With Check Point Full Disk Encryption, the cost is \$75,000. The difference of \$825,000 is how much an organization would





potentially save with Check Point Full Disk Encryption. Dividing \$825,000 by 52 weeks yields a rate of \$15,865 per week per 1,000 seats. By cutting a six-month deployment in half to 13 weeks, Check Point Full Disk Encryption would therefore reduce security exposure by \$206,245 per 1,000 seats.

For a complete discussion of other factors on TCO, see the Check Point Guide to the TCO of Encryption.

Learn more

Please contact Check Point for more information about the economics of rapidly deploying our Check Point Full Disk Encryption product in your organization's IT environment. We encourage your organization to perform its own cost-of-risks analysis by adapting the table on page 6. Your organization may also request a copy of our white paper titled, Guide to the TCO of Encryption. Please contact your Check Point partner sales representative, or visit www.checkpoint.com.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSP, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.