



# Federal Guide to the Value of Encryption

Encryption from Check Point can reduce recurring financial risks of security exposure by 90 percent

# Contents

- Executive summary ..... 3
- Gauging financial risks of information loss ..... 4
  - Replacement costs ..... 4
  - Recovery costs ..... 4
  - Effect costs..... 5
  - Reputation 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 by 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 federal organizations must also address the risk of losing portable computing devices that contain sensitive data.

Surveys indicate that up to 60 percent of information theft results from lost or stolen equipment, while only 25 percent results from network intrusion. 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 files 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 is about the economics of encryption. It assesses financial risks to information loss if a federal government agency or department does not use encryption and how those losses can be reduced by using encryption. By using Check Point Endpoint Security™ encryption solutions, federal organizations can cut the annual costs of security exposure resulting from the loss or theft of computing equipment by 90 percent or more.

“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 agencies when computing equipment with federal information is lost or stolen. These costs include replacement, recovery, effect, and reputation. Some of these costs are straightforward, such as the price of a computer or software. Others may vary by agency, pertinent regulations and associated penalties, and other conditions. The following describes these variables and how they may be affected in scenarios with and without encryption. Agencies may adjust these variables as they uniquely affect their 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 federally owned devices. According to a survey by Check Point, travelers left 85,000 cellular 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 the 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?”

**FBI report.** An agency representative will need to gather and provide pertinent information to the FBI or other law enforcement agencies, 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.

**Insurance claims.** The insurance claim process entails many of the same items as a police report. An agency 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.

**Employee downtime.** The agency employee or contractor 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 revenue-driven activity, such as collection of taxes or user fees.

**Assessment of exposure.** The agency security team will need to assess the effect of exposure due to the potential release of sensitive federal information. The effect will grow if the loss or theft includes personally identifiable information of employees or other individuals—especially if it is subject to regulation and personal privacy laws. Assessment is the largest expense 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 to effect or reputation costs as described below. Encryption will also help agency and department managers and executives responsible for information security to avoid potential civil and/or criminal investigations and charges related to the exposure of personally identifiable information.

### Effect costs

Effect 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.** Federal agencies and departments are required to implement safeguards for information security as prescribed by the Federal Information Security and Management Act (FISMA). On June 23, 2006, the president’s Office of Management and Budget (OMB) issued a memorandum for heads of departments and agencies concerning the protection of sensitive agency information. The memo provided a checklist for protection of remote information based on security controls specified in the National Institute of Standards and Technology’s (NIST) Special Publication 800-53. In addition to using the NIST checklist, OMB recommended that all agencies and departments “encrypt all data on mobile computers/devices that carry agency data, unless the data is determined to be non-sensitive.” Many federal regulations and laws require agencies and departments to protect customers or individuals’ personally identifiable information and 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 agencies that suffer data breaches of personally identifiable information to notify affected users about the incident. Meanwhile, security breach legislation was 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.

“The top-level encryption of the Check Point Endpoint Security 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

**Account changes.** Exposure of personally identifiable information can require an agency to change users to new accounts, which can trigger large administrative charges for incidents involving thousands of people.

**Credit checks.** An agency 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 people affected by the disclosure of data.

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

**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 to data loss.

**Effect 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 agency from notification if the lost or stolen data was encrypted.

### Reputation costs

The value of reputation is “priceless.” It is difficult to precisely gauge how a president’s administration, Congress, or the public will react to news that federal data has been lost or stolen. Reputations will suffer and responsible administrators may lose their jobs. In the wake of a data breach, hearings may be held, and it is possible for sanctions to occur, including difficulty in obtaining future appropriations from Congress. Also, class-action lawsuits and regulatory penalties may result from the same news. 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 equated with a loss of reputation can be prevented by using encryption.

### Typical costs and ROI with encryption

The financial risks of security 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 encryption can eliminate 90 percent or more of the annual cost of risk caused by unintended exposure of federal or personally identifiable information on lost or stolen devices.

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

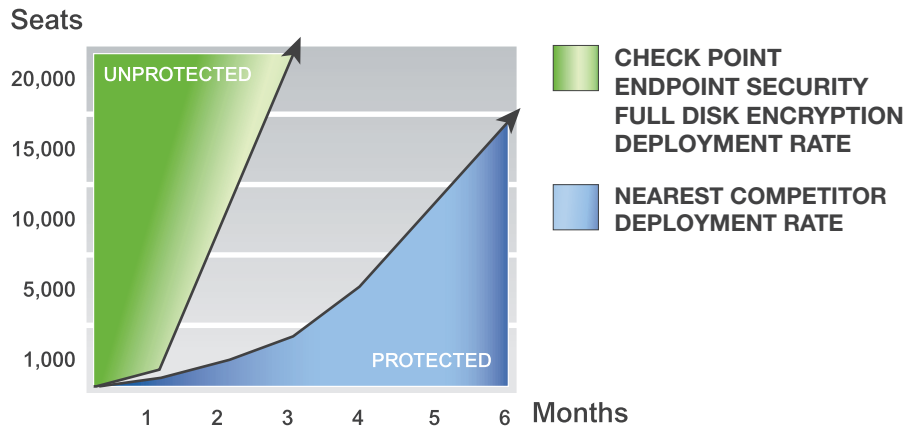
Cost element	Typical cost range (per incident)	Unprotected scenario	Protected scenario
<b>Replacement—</b> Lose equipment?	\$1,000 – \$3,000	\$1,500	\$1,500
<b>Recovery—</b> Know what information is on the lost system?	\$2,000 – \$10,000	\$6,000	\$1,000
<b>Effect—</b> Know what laws subjected to?	\$15,000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

**Total cost of ownership**

The other side of return on investment is the total cost of ownership (TCO) for encryption. One element of TCO is how fast an agency or department can eliminate the recurring cost of the risks detailed above. The longer it takes to deploy encryption, the more a federal 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 organization. Typical deployments for a large agency of tens of thousands of seats can require six months or more. Check Point encryption solutions deploy much faster than competing products, based on the experience of replacing those products on hundreds of thousands of seats around the world.

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

An agency can calculate the economic value of superior deployment capability of Check Point 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 white paper, Guide to the TCO of Encryption.

## Learn more

Please contact Check Point for more information about the economics of rapidly deploying Check Point encryption solutions in a federal organization IT environment. We encourage your agency or department to perform its own cost-of-risks analysis by adapting the table on page 7. Your federal organization may also request a copy of our white paper titled, Guide to the TCO of Encryption. Please contact a Check Point partner sales representative or visit [www.checkpoint.com](http://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](mailto: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, SmartLSM, 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.