



## Finding Value in a Turbulent Economy with PCI DSS

July 2010

*Prepared for WatchGuard Technologies by ReymannGroup, Inc.*

In these turbulent economic times, many merchants are struggling to survive. However, the need to secure cardholder data and comply with the PCI DSS mandates is not going away.

The list of merchants that have experienced a breach in the security of credit card data continues to grow.<sup>1</sup> The frequency of these data loss events, mounting financial losses, and systemic fear created among consumers are driving a new awareness of the relevance and importance of the Payment Card Industry Data Security Standards (PCI DSS) and proactive information security and risk management practices for merchants. The threat of a data breach to your organization and the subsequent damage to your customers and company are real.

However, the task of complying with the PCI DSS mandates and securing cardholder data can be a daunting project for most merchants. PCI DSS defines detailed technical, physical, and administrative mandates.

Taking no action is not an option. Partial compliance is not an option. PCI DSS offers only two alternatives – Pass or Fail. If you do not meet all of the requirements that apply to your organization, you fail.

While implementing a compliant security program is a significant challenge, the alternative cost of a data breach or paying fines<sup>2</sup> and penalties for non-compliance can result in bankruptcy.

Hence, the struggle! While most merchants recognize that they must ensure compliance and protect cardholder data, they may not have access to the necessary expertise or resources. For example, gathering information to prepare for an audit and the annual self-assessment adds to the existing workload and distracts from other revenue generating projects.

---

<sup>1</sup> Forever 21, Polo Ralph Lauren, Sams Club/Walmart, DSW, RBS Worldpay, TJX, Heartland Payment Systems - to name a few - have all experienced breaches.

<sup>2</sup> The card association rules are the authority that allows for fines to be levied and to require each merchant to abide by the PCI DSS. Most merchant bank “operating guides” state that the merchant agrees to all card association rules.

In this paper, we define the value of PCI compliance and the cost of non-compliance. We also offer a strategy and tools that will help you to cost-effectively meet the intent of the PCI DSS mandates – creating a day-to-day culture of proactive and real-time information security throughout your organization and infrastructure. Assuming that most readers already have a general understanding of the PCI DSS mandates, our goal is to provide a forward-looking perspective on how you can:

- Leverage the right technology to help reduce the cost of your compliance efforts
- Simplify your recurring activities for pre-audit reviews, annual self-assessments, and monthly attestation
- Enable security of your customer’s credit card data

Whether you are a Level 1, 2, 3, or 4 merchant, this paper offers insights and tools to help you cost-effectively prepare for your next audit, complete the self-assessment questionnaire, protect cardholder data, and enable successful PCI compliance and security.

## Think about it:

1. How loyal are your customers - Will customers stay with you in the event of a data breach?
2. What is the cost of gaining a new customer?
3. Do you know the cost of responding to the following type of class action lawsuit?  
“...this action arises from Defendant’s failure to maintain adequate computer data security of customer credit and debit card data, which was accessed and stolen by a computer hacker... Because of Defendant’s actions, millions of its customers have had their personal financial information compromised, have had their privacy rights violated, have been exposed to the risk of fraud, and have otherwise suffered damages.”<sup>3</sup>
4. Do you have in-house resources and expertise to perform PCI DSS self-assessments and prepare for outside audits?
5. Did you know that there are technology solutions available to help you cost-effectively simplify your PCI compliance and data security initiatives?
6. Did you know that a firewall, encryption, and a zoned network help establish a foundation for PCI compliance and good security?

## Credit Card Data Security Is the Primary Focus

The security of cardholder data and any network component, server, or application that is included in or connected to the cardholder data environment is the primary focus for the PCI DSS. Specifically, PCI DSS v1.2 states:

- The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.
- Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.
- Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
- Applications include all purchased and custom applications, including internal and external (Internet) applications.

---

<sup>3</sup> Doherty-v-Hannaford: Plaintiff’s Class Action Compliant and Demand for Jury Trial, 03/19/2008.

In general, all merchants are required to complete an annual PCI audit with a qualified security assessor (QSA) or self-assessment questionnaire and perform a quarterly scan of its network scans by an approved scanning vendor (ASV).<sup>4</sup>

However, as merchants such as Hannaford Bros. and others have found, compliance with these annual and quarterly processes is not sufficient. Compliance does not always ensure security. The hackers and other cyber criminals are not initiating annual or quarterly attack strategies – their means of delivery and types of attacks are constantly evolving.

This is why PCI DSS should not be viewed as an annual or quarterly point-in-time project. The PCI Security Standards Council<sup>5</sup> recognizes the need to constantly evaluate the adequacy of the compliance criteria and amend them, as needed. For example, in October 2008, they published updates to clarify and strengthen several of the standards. Some key updates include the clarification that under:

- *Requirement 1* - Configuration requirements apply to both routers and firewalls. It now has added flexibility to allow for a review of firewall and router rule sets to “at least every six months” so that controls can be customized to an organization’s risk management policies.
- *Requirement 2 & 4* – PCI DSS applies to wireless environments that are “attached to the cardholder environment or transmit cardholder data.” Wired Equivalent Privacy (WEP) will no longer be acceptable (WEP is prohibited on new wireless implementations after March 31, 2009. WEP is prohibited for current wireless implementations after June 30, 2010). You will need to use strong encryption technologies for wireless networks, for both authentication and transmission such as WPA or WPA2. SSIDs may now be broadcast. Since the SSID is broadcast over numerous other messaging and communication channels, disabling SSID broadcast does not prevent malicious users from determining the SSID.
- *Requirement 5* – Anti-virus software or programs apply to all operating systems that are commonly affected by malicious software, if applicable anti-virus technology exists.
- *Requirement 11* - Added additional focus on testing for the presence of rogue wireless access points and implementing wireless IDS/IPS. Clarified that qualified internal personnel and external third parties can perform penetration tests.
- *Requirement 12* - Clarified that employee acknowledgement of the security policies and procedures must be done at least annually and in written or electronic form.

So if you thought the PCI DSS mandates might some day go away – think again. They are here to stay and will continue to change over time to keep pace with the dynamic nature of cyber-security threats to cardholder data. Therefore, it is imperative that each merchant understand how to translate today’s compliance mandates and security challenges into recognizable value for the organization.

## How Will PCI DSS Affect Your Key Business Objectives?

We encourage all merchants to instill a culture of security and an infrastructure that supports protection of cardholder data and keeping pace with the compliance mandates. This proactive strategy will create benefits that offset and outweigh the costs of adopting data security practices and implementing the right technology solutions to help. It will also help organizations to avoid a material event such as a data breach of cardholder data that could result in substantial fines, penalties, financial loss, and possible bankruptcy.

For example, let’s compare and contrast two companies. Company A has implemented an effective PCI DSS program. Company B has not. The executive management team at both companies agrees that key business

---

<sup>4</sup> Level 2, 3, and 4 merchants are required to successfully complete an annual PCI DSS Self-Assessment Questionnaire, in addition to a quarterly network scan with an approved scanning vendor. Level 1 merchants are required to complete an annual onsite review by an internal auditor or qualified security assessor, in addition to the quarterly network scan.

<sup>5</sup> The PCI Security Standards Council is responsible for management and dissemination of the PCI DSS.

objectives include: customer trust; strong brand and reputation; minimal liability; business longevity; enterprise security; and efficient operations.

In Table 1, we have summarized the affect of compliance versus non-compliance on these business objectives for each company, respectively.

Objective	Company A – PCI Compliant	Company B – Non-Compliant
<b>Brand Reputation Customer Trust</b>	PCI Compliance: <ul style="list-style-type: none"> <li>- reduces likelihood of lost customers and revenues from a breach</li> <li>- re-enforces customer trust, brand, reputation</li> <li>- promotes excellence, customer service, growth</li> </ul>	After a breach: company’s stock price falls, its image is tainted even further by the press, and customers migrate to competitors. According to research by the Ponemon Institute in its <i>2008 Annual Study: Cost of a Data Breach</i> , 31% of customers leave after a breach.
<b>Limit Liability Business Longevity</b>	If a merchant experiences a breach while compliant, “Safe Harbor” protects the merchant from fines and compliance exposure. Safe harbor provides members protection from Visa fines in the event its merchant or service provider experiences a data compromise. To attain safe harbor status: (1) A member, merchant, or service provider must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation. (2) A member must demonstrate that prior to the compromise their merchant had already met the compliance validation requirements, demonstrating full compliance. (3) The submission of compliance validation documentation, in and of itself, does not provide the member safe harbor status. The entity must have adhered to all the requirements at the time of the compromise	PCI non-compliance and weak or no security measures can negatively affect your bottom line and eventually cause bankruptcy. Credit Card Association or Merchant Bank fees and class action lawsuits are only the tip of the iceberg. Add the cost of legal counsel, identity theft protection for customers, customer notification, negative publicity, rebuilding reputation, and loss of customer loyalty. Even the healthiest of businesses will be stressed. In its <i>2008 Annual Study: Cost of a Data Breach</i> , the Ponemon Institute reported that the total costs of a data breach continue to increase. The total average costs of a data breach grew to \$202 per record compromised. This is an increase of 2.5 percent since 2007 (\$197 per record) and 11 percent compared to 2006 (\$182 per record).
<b>Enterprise Security</b>	PCI compliance: <ul style="list-style-type: none"> <li>- Forces you to become aware of the strengths and potential gaps in security practices.</li> <li>- Helps you detect, prevent, and respond to threats to your information.</li> <li>- Is a catalyst for enterprise-wide security. Implementing and maintaining compliant PCI DSS policies, practices, and technology can jumpstart a culture of security in your employees and throughout the organization.</li> </ul>	Non-compliance and weak or no security frequently equates to an increase in the likelihood of a security breach and loss of credit card data. Subsequently, such events could result in fines, penalties, damaged reputation and brand, lost customers, and bankruptcy.
<b>Efficiency</b>	<ul style="list-style-type: none"> <li>- PCI compliance creates a best practice operating environment that helps avoid downtime and disruptions in the delivery of service to customers and employees.</li> <li>- Automated solutions will help streamline and reduce the cost of PCI compliance.</li> <li>- The right technology makes it easier to prevent, identify, and respond to possible threats. Such technology includes firewalls, unified threat management solutions, network monitoring, encryption, event identification, and reporting.</li> </ul>	Non-compliant companies face possible restrictions and the loss of credit card processing privileges. They are also more susceptible to data loss incidents. If a security breach occurred it would disrupt business and halt productivity. Key resources would be redirected away from revenue generating projects to respond to the incident

As you continue to plan for the necessary budget and resources to accomplish your business objectives, comply with the PCI DSS mandates, and ensure the security of cardholder data, consider the following check list tool to help you itemize the benefits and costs of PCI compliance for your organization. We encourage you to leverage some or all of the items in this checklist to facilitate a meaningful cost-benefit discussion within your company.

# PCI DSS Compliance Cost-Benefit Checklist

## BENEFITS OF COMPLIANCE

**As a company, our goal is to:**

- Avoid fines.** If we were fined, what is the maximum dollar amount that we have in reserve for such contingencies?
- Establish and reinforce trust** with our customers.  
Have we announced or published our formal commitment to customer privacy and security?  
- Brick-n-mortar and on-line customers expect credit card data privacy and safety.
- Avoid customer churn.** What is the cost of acquiring a new customer? What is the cost of keeping a current customer?
- Save time and expense.** Automating PCI compliance streamlines the process and simplifies recurring requirements for monthly attestation and audit and forensics reporting.
- Create efficiency.** An operating culture of security avoids downtime and disruptions in delivery of service.
- Secure all sensitive data, not just cardholder data.** Cardholder data security practices can be easily applied to other areas of the organization.
- Become a more secure company.** Instituting good security practices in one area can potentially help secure other areas.
- Comply with other federal and state laws.** Compliance with PCI DSS mandates enables cost-effective compliance with many other federal and state data security laws and regulations.

## CONSEQUENCES OF NON-COMPLIANCE

**As a company, we want to avoid:**

- Data security breach**
  - Would we know if sensitive data was leaked? Do we have a means to know or will our customers notify us after the fact?
  - How long would it take us to respond? (hours, days, weeks, months?)
  - What is the average cost per record for us to respond? Estimated at \$202 per customer record for most companies. (How many records do you have? Do the math!)
- Loss of processing privileges**
- Reputational loss**
- Damage to brand**
- Customer churn**
- Financial loss**
  - Credit Card Association or Merchant Bank fines and penalties
  - Liability (e.g., civil suits)
  - Identity theft protection expense for affected customers
  - Loss of revenue. Lost customers. Allocation of resources to respond to the event and ongoing reporting and follow-up work with auditors, lawyers, forensics, customers, and press.
  - Cost to rebuild customer base and reputation

If you experience a breach of customer credit card data, it will be a struggle to survive. The liabilities and hard costs are staggering and could drive many merchants to bankruptcy. For example, consider your ability to recover from the financial implications of a data breach.

The following examples show that the risks and financial exposures are real.

#### **ChoicePoint**

- January 2006, \$15 million settlement with the Federal Trade Commission
- January 2007, \$10 million class action lawsuit

#### **TJX**

- Expenses associated with the data breach are estimated at \$500 million to \$1 billion
- TJX agrees with VISA to pay \$40.9 million into a fund for handling VISA customer losses from the breach
- TJX sets aside a reserve for future costs related to the breach of \$107 million and \$256 million for VISA and MasterCard, respectively
- TJX has at least 19 law suits pending, plus an ongoing Federal Trade Commission investigation, and 37 State Attorney General investigations

While these larger enterprises are still operating and able to respond to these unfortunate events, most merchants do not have their financial capacity and will struggle to avoid bankruptcy.

## **Do Not Wait to Find Out If You Pass or Fail**

PCI compliance is not simply a requirement; it can differentiate success from failure. By proactively implementing best practice strategies for PCI compliance and security across the entire business and network, organizations establish the parameters needed to:

- Deliver on their customer promise of trust, protect data privacy, and security
- Reduce liability risk
- Improve the effectiveness of their operations
- Avoid disruptions in service and operations
- Demonstrate continuous compliance

As a starting point to help merchants plan how to best accomplish PCI DSS compliance and security, we offer the following recommendations for each merchant to consider. While this list does not cover everything that you may need to consider, it highlights several best practices that will help.

#### **Conduct Self Assessments**

We recommend that each merchant leverage in-house expertise or partner with knowledgeable outside resources to perform a pre-audit review (for Level 1 merchants) and preliminary self assessment (for Levels 2, 3 & 4 merchants). Performing this work before the annual onsite audit or formal self assessment is a cost-effective means of identifying your strengths and weaknesses early – allowing you time to correct any deficiencies before you have a formal audit or assessment.

#### **Select the Right Technologies**

Achieving a secure and compliant culture goes beyond a “CHECK THE BOX/YES/NO” self-assessment audit methodology for compliance. All merchants that complete the annual self-assessment questionnaire and quarterly security scan of their network need to understand the full intent of the questions that are presented. Each merchant cannot successfully complete the self-assessment questionnaire unless it has established a technology infrastructure that enables the company to address the real intent of the PCI DSS requirements – doing what is right to protect the company, its assets, and its customers.

PCI compliance requires governance over your entire IT infrastructure. Thus, it is imperative that you use technologies that address your entire network, all the data components as well as all the systems that host PCI data. This allows you to achieve a broader approach to your compliance initiatives and provide maximum protection for cardholder data. Example technology strategies that must be implemented include:

- Installing and maintaining secure firewalls
- Encrypting across open, public networks
- Establishing a zoned network architecture
- Tracking and monitoring all access to the network and cardholder data

By automating and centralizing as much of the PCI compliance processes and technologies as possible, you ensure agility with operating efficiency, and relieve resources to focus on revenue generating initiatives. This empowers employees, makes the processes more manageable, and uses less time and capital to enable compliance.

#### **Team with Strategic Technology Partners**

Hiring consultants to perform security audits is not a cost-effective option, by itself. Constant changes throughout your network and in the nature of the threats to your network and data require you to partner with strategic technology companies that provide automated and real-time security. You need to plan beyond the annual audit or self-certification and establish an ongoing risk-assessment culture that will enable you to maintain your strengths identified in the audit or self-certification and correct any weaknesses. Outsourcing for technologies that deliver firewall, encryption, and real-time monitoring of your network is a cost-effective alternative to help you establish and maintain a secure and compliant infrastructure.

#### **Appoint a Champion - Make it more than just an annual compliance project**

One of the most valuable practices a business could undertake would be to create a sustainable, repeatable process. PCI compliance is not a point-in-time activity – it is a continuous process. Implementing formal security processes, policies and procedures and ensuring that these are followed does much more than simply satisfy the card association mandates - it lessens the likelihood of losing cardholder data.

Each organization should designate an individual or group with the authority and responsibility to champion the security and compliance culture. This individual should understand and stay abreast of the legal, regulatory, and other requirements, the controls needed to meet them, and actively pursue the right solutions that resolve any security issues. Your security point-person can then propagate security throughout your enterprise with an employee awareness program to educate your staff on how cardholder data should (and should not) be handled.

### **WatchGuard® Enables Continuous Self-Assessment and PCI Compliance**

Organizations must find a solution that allows them to address a broad range of PCI compliance requirements. This enables them to streamline their security initiatives. No one solution will be the answer, however finding a multi-layered solution brings new levels of efficiency to their security efforts. WatchGuard Technologies delivers a wide range of solutions designed to help businesses address PCI compliance and security as a whole. With WatchGuard as a strategic partner, businesses can employ a culture of security within their organization.

WatchGuard capabilities align with PCI compliance requirements and include the following:

#### **Streamlining Self Assessments**

The WatchGuard *PCI Self Assessment Questionnaire (SAQ)* tool automates and streamlines the self-assessment process and monthly attestation process. It includes all of the PCI DSS self-assessment questions and applicable testing procedures and aligns them against the specific WatchGuard solution capabilities, where applicable. The tool also allows customers to fill in the non-WatchGuard requirements to prepare a complete self-assessment as supporting documentation for the merchant's monthly attestation of PCI DSS compliance.

## WatchGuard SAQ Tool Sample Screen Shot

<b>Build and Maintain a Secure Network</b>			
<i>Requirement 1: Install and maintain a firewall configuration to protect data</i>			
	<b>Question</b>	<b>Yes</b>	<b>No</b>
In addition to the WatchGuard capabilities, additional reviews should be performed on firewall configurations and other like systems outside of the WatchGuard capabilities.			
<b>1.2</b>	<p>Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder environment?</p> <p>Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, or which is out of the entity’s ability to control or manage.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Test Procedure:</b></p> <p>Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment.</p> <p>The <u>WatchGuard</u> XTM proxy architecture is ideal for meeting these requirements. The proxy architecture provides detailed control over which protocols, ports and content are allowed through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy that allows only approved traffic to pass into the cardholder data environment. The XTM IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.</p>			
<b>1.2.1</b>	<p>Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p><b>Test Procedure:</b></p> <ol style="list-style-type: none"> <li>a. Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.</li> <li>b. Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement</li> </ol> <p>The WatchGuard XTM proxy architecture provides granular control over which protocols, ports, and content are allowed through the firewall. Using the XTM proxy technology will block ALL traffic except for that explicitly defined by the user.</p>			

### **Building and Maintaining a Secure Network**

The WatchGuard XTM proxy architecture provides detailed granular control over which protocols and content are allowed through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy that allows only approved traffic to pass into the PCI DSS operating environment.

The XTM Intrusion Prevention and Gateway AntiVirus services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts. WatchGuard’s zoned network architecture allows its firewalls to be configured so that traffic from the Internet into the public-facing servers in the DMZ, and from the DMZ into the trusted zone, is restricted to approved traffic types only.

This also ensures that none of the IP addresses in the trusted zone are visible or accessible from the Internet. In addition, WatchGuard System Manager may be used to define and deploy a synchronized configuration to each XTM device that will then be applied during the startup of each appliance.

### **Protecting Cardholder’s Personal Data**

PCI DSS requires the use of a zoned network architecture to segregate cardholder data so that it cannot be accessed directly via the Internet. WatchGuard XTM appliances support network zones, and they can be configured to create a DMZ for all public-facing servers and a Trusted zone where the cardholder data resides.

In addition, all management communications with XTM appliances are done via a secure encryption-based protocol and all XTM appliances support IPsec and SSL VPN communication.

WatchGuard also helps protect cardholder data over wireless networks. Wireless networks are inherently unsecure, but there are some circumstances where they cannot be avoided. In these cases, PCI compliance requires that the wireless operating environment be physically segregated from the wired environment and appropriately firewalled. When a Wi-Fi solution must be used, the XTM 2 Series supports WPA2 and can be combined with either an IPsec or SSL VPN to achieve compliance and protect credit card data.

#### **Maintaining a Network Vulnerability Management Program**

WatchGuard's unified threat management (UTM) solutions provide comprehensive network protection. They integrate application proxy firewall, zero day attack prevention, anti-spyware, anti-virus, anti-spam, intrusion prevention, and URL filtering on a single platform. This greatly reduces the time and cost associated with managing multiple point solutions and significantly improves protection from blended threats.

The solution provides gateway anti-virus support that reduces the ingress of malware into the network. Its automatic updates of the Gateway AntiVirus signature database works to protect the network from vulnerabilities. In addition, WatchGuard updates the appliance Logs whenever traffic is denied by the Gateway AntiVirus and whenever the signature sets are updated.

WatchGuard XTM provides an additional layer of protection. The HTTP/HTTPS proxy is a high-performance content filter that examines web traffic to identify suspicious content, which can be a virus, spyware, or other type of intrusion. It can also protect your web server from attacks from the external network.

#### **Implementing Strong Access Control Measures**

XTM appliances deliver stringent access controls with their two-factor authentication, including RADIUS, SecurID, and individual VPN certificates. They also support authentication via Active Directory, which streamlines authentication, saving time and eliminating hassles. Organizations can implement strong controls with an XTM device as it stores all password information in an encrypted format. This provides an additional layer of security. Furthermore, WatchGuard SSL 100 and SSL 560 appliances make secure remote access easy and affordable, regardless of the network size.

#### **Regularly Monitor and Test Networks**

WatchGuard helps monitor networks by tracing each login activity to an individual. All XTM appliances support authentication via Active Directory.

### **Take the Next Step**

With WatchGuard Technologies deployed throughout your enterprise, you help enable compliance and create a culture of security within your organization. For a copy of the WatchGuard *PCI DSS Self-Assessment Questionnaire* tool and to learn more about WatchGuard and how they can help your business, call 1.800.734.9905 for a salesperson who will guide you through a solution that best fits your needs, or go to [www.watchguard.com](http://www.watchguard.com) to sign up for a free trial.



**ADDRESS:**  
505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

**WEB:**  
[www.watchguard.com](http://www.watchguard.com)

**U.S. SALES:**  
+1.800.734.9905

**INTERNATIONAL SALES:**  
+1.206.613.0895

**ABOUT WATCHGUARD**

Since 1996, WatchGuard Technologies has provided reliable, easy-to-manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit [www.watchguard.com](http://www.watchguard.com).



**ADDRESS:**  
1908 Blue Ridge Road  
Edgewater, MD 21037  
USA

**WEB :**  
[www.reymanngroup.com](http://www.reymanngroup.com)

**CONTACT:**  
Phone: (410) 956 7336  
Fax: (410) 956 7338  
Email: [info@reymanngroup.com](mailto:info@reymanngroup.com)

**ABOUT REYMANNGROUP**

ReymannGroup, Inc. provides finance, healthcare, energy, public sector, and retail subject matter expertise. Our firm helps companies evaluate their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly-qualified professionals, authors of regulations and books, and subject matter experts familiar with industry regulations and best practices.

---

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. © 2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. WGCE66621\_071910