CYBERSHARK™

CYBERShark WHITE PAPER

ESSENTIAL PRACTICES FOR ACHIEVING SECURITY COMPLIANCE MANAGEMENT

Security is everyone's concern, but it's our business.

WWW.CYBERSHARKINC.COM

CONTENTS

CYBERSHARK™

1

EXECUTIVE SUMMARY

Security compliance management is the process of creating a successful security infrastructure and compliance culture. To do this requires the right people, policies, and technology to be in place and for an entire organization to recognize and appreciate the need to achieve security compliance. The problem in creating this "compliance by default" environment is a thorny one. With the ever changing landscape of IT security threats and compliance mandates, the work to ensure compliance can become overwhelming.

In recent years, dramatic changes in the trends of information security threats have pressured organizations – particularly large corporations and medium-sized businesses – to develop new and more proactive strategies for mitigating security risks.

Protecting the network perimeter is no longer enough. With threats like data theft on the rise, companies must now preserve the safety of critical corporate assets across the organization from the perimeter to the deep core where important confidential data resides. The challenge is that few IT environments are static. Most are rapidly expanding in breadth and complexity to keep up with business requirements. This growth has the byproduct of also increasing the organization's digital attack surface, a problem only made more complex by the virtual explosion of legislation regarding the privacy and security of information. The synergistic effect of these combined problems and the evolving nature of cyber threats is having a profound effect on organizations as they struggle to both protect themselves and their customers from cyberattack, while also protecting themselves from the regulatory mandates that govern their business and their confidential data.

EXECUTIVE SUMMARY (CONTINUED)

To cope with this change, more and more businesses are adopting comprehensive real-time monitoring technologies. Services such as SIEM allow IT and security compliance professionals to keep a close eye on an organization's devices, databases, systems and applications. Combined with intelligent log management processes for collecting, documenting and storing log data, security teams can start to dig their way out of most of the pitfalls surrounding security compliance management.

With the right technologies, security policies, and resources in place, organizations of all sizes and industries can establish an optimal approach to information security that manages risk and strengthens security posture. By doing so, companies can achieve, maintain, and prove regulatory compliance.

Security compliance management makes regulatory compliance achievable – when organizations take action to identify and implement the essential practices needed to protect the confidentiality, integrity, and availability of valuable corporate assets and information.

2

THE COMPELLING ARGUMENT FOR A PROACTIVE SECURITY COMPLIANCE PROGRAM

Today's organizations face unprecedented challenges in battling security threats, keeping up with changing technology environments, and maintaining compliant business operations. Not only must companies figure out a way to do all of this cost effectively they often have to make due with while entrusting corporate security postures to the expertise of available resources.

In the early days of the Internet, threats like worms and viruses made their way through the network perimeters of organizations around the world. For most, these early attacks were more digital harassment than true threats. That has changed significantly. Today, headlines about IT security breaches read very differently. With the expansion of the Internet of Things and the more interconnected our businesses and lives become, the greater the threat from cyberattack has grown. Nation states actors, organized crime syndicates and idealistic "hacktivists" have catapulted cybersecurity onto the global stage. Profit-driven attackers leverage an unbelievable breadth of extremely complex attack methodologies coupled with more sophisticated social engineering angles to prosecute their attacks. Intruders are more successful and their targets are often breached and compromised for months – even years – before beingdetected.

According to the Verizon 2015 Data Breach Report, companies are struggling to maintain security positive postures. More than 99.9% of the published vulnerabilities in operating systems, hardware and application software can be found to have been exploited by attackers more than year after the vulnerability is published. Worse, IBMs 2015 Cyber Security Intelligence Index reports that more than half of the data breaches we know about are caused by corporate insiders, including employees, third party contractors and partners. The costs associated with these data breaches is staggering. According to SpectorSoft's 2014 Insider Threat Survey, U.S. companies reported $40 billion in losses from insider based attacks alone.

(continue)

THE COMPELLING ARGUMENT FOR A PROACTIVE SECURITY COMPLIANCE PROGRAM (CONTINUED)

Worse, the threat is only going to continue to grow. A PWC survey of 9700 companies found that they'd detected nearly 43 million security incidents in 2014, a number that reflects a compound annual growth rate of 66%.

In 2015, 700 million records were compromised. The price tag for these loses is estimated at $400 million states the Verizon 2015 Data Breach Report. The problems don't stop after the attack, either. When companies fall short in protecting data, they can lose customer confidence and find themselves targets legal action.
The grim reality is that vulnerabilities exist in every organization, regardless of size. Yet an increase in the complexity of today's technology environments makes it increasingly difficult for companies to understand where security vulnerabilities lie. Often, companies do not have the security expertise to adequately mitigate risk, or they lose that expertise during resource reductions. Businesses need end-to end, real-time visibility into every aspect of security, Security information is scattered across the organization with nothing to converge physical and logical security into a single, unified effort and view.

Companies must turn to a new level of technology and automation to prevent attacks, and especially data-centric attacks, from wreaking havoc within the organization. All security-related information must be monitored, aggregated, and processed to empower companies to identify vulnerabilities, watch for attacks, and provide tangible evidence of security efforts in the event of regulatory audits. By establishing and implementing optimal security practices based on individual circumstances, companies can not only strengthen security postures, but can also meet regulatory compliance.

3

COMPLIANCE: A "BY-PRODUCT" OF IMPLEMENTING OPTIMAL SECURITY

Regulatory pressures vary to some degree by industry and regulation, but in general, they can be dealt with by tailoring an information security program and architecture to provide the necessary elements of risk management, policy development, active monitoring, incident response, documentation, reporting and organizational security awareness. Though no one product or mechanism can serve as a complete information
security solution, maintaining an acceptable level of risk can be achieved. Through a combination of program and process elements, effective management and expertise and use of the right tools, security compliance management can ensure
compliance success. This means that publicly-held organizations that maintain electronic protected health information (ePHI) can meet HIPAA and Sarbanes-Oxley requirements and retail companies that process credit card information can better meet
PCI-DSS mandates.

Most laws, regulations, and guidelines identify common IT security practices that help to establish a continuous security compliance management program. While these requirements may apply to different industries and government, the mandates are based on a common foundation of recognized best-practice risk management principles. These "common security compliance threads" that help secure corporate assets and information while enabling them to meet compliance are listed in
Table 1.

(continue)

COMPLIANCE: A "BY-PRODUCT" OF IMPLEMENTING OPTIMAL SECURITY (CONTINUED):

THE 15 COMMON SECURITY COMPLIANCE THREADS

Risk Assessment	Maintain an ongoing information security risk assessment program, providing the necessary visibility into the infrastructure to assess and manage risk on a real-time and historical basis.
Access Controls	Only allow access for authorized individuals and devices and disallow to all others.
Sensitive Data Protection	Implement administrative, technical, and physical safeguards to protect sensitive nonpublic corporate information and private customer data.
Vulnerability & Threat Assessment	Perform periodic network scans to identify vulnerabilities.
Firewalls	Establish a firewall policy that states management's expectation for how the firewall should function as a component of the overall security policy. The firewall selection and policy should stem from the ongoing security risk assessment process.
IDS & IPS	Implement IDS and IPS capabilities to help detect, prevent, and respond to intrusion activities.
Patch Management	Ensure that patch management standards include procedures for identifying, evaluating, approving, testing, installing, and documenting software patches.
Change Management	Fully authorize, track, and document all security policy and process changes.
Configuration Management	Develop baseline standards that define the original versions for hardware, software, services, documentation, and security settings. Then evaluate, approve, document and disseminate all changes to baseline versions.
Logging	Take reasonable steps to ensure that sufficient data is collected from secure logs files on all network devices and critical applications. Then identify and respond to security incidents and monitor and enforce policy compliance.
Monitoring	Actively gather and analyze data in real-time on new threats and vulnerabilities, actual attacks, and the effectiveness of their security controls.
Reporting	Report on the status of information security and security events. Such materials include matters related to the adequacy of internal controls, risk management and control decision, security breaches, and other events that could negatively affect shareholder value of the customer.
Rapid Response	Identify that a material event (such as negatively affecting shareholder value or the customer) has occurred, assess the effect on the company and customer, take remedial action, and notify appropriate parties such as customers, regulators, and shareholders. The Securities and Exchange Commission has specified a "48-hour" response, while other regulatory bodies have specified a "reasonable" amount of time.
Intrusion/Incident Response	Establish a formal response program based on the full cycle of incident management: event detection, evidence collection and archiving, ticketing, prioritization, mitigation, and resolution as events occur. This minimizes damage to the operation and customers through containing the intrusion, restoring systems, and providing assistance where needed.
Business Continuity	Facilitate business continuity through management documenting, maintaining, and testing the business continuity plan and back-up systems on a periodic basis to mitigate the risk of system failures and unauthorized intrusions.

Understanding these common security compliance threads enables organizations to adopt a more proactive and cost- effective security compliance management initiative. A key success factor for enabling compliance with these common threads is an organization's ability to select and adopt the right technology to address a broad range of these mandates. Done right, security compliance management leverages the best resources, the right technology solutions, and prudent practices to foster a culture of ongoing security risk management. As a result, achieving compliance becomes a "by-product" of implementing optimal security management.

CYBERSHARK™

4

THE IMPORTANCE OF MONITORING DEVICES, DATABASES, SYSTEMS, AND APPLICATIONS

The relative value of information assets is unquestionable. Unfortunately, the threats to the confidentiality, integrity, and availability of those assets are ongoing. The vulnerability of the systems and architecture that store and carry those assets ultimately determines whether those assets will be compromised. To ensure that systems, processes, and personnel are aligning with security compliance management policies in place to protect valuable corporate assets, organizations must be able to assess and manage risk. Most regulations in fact demand that risk assessment and management function as the leveraging a powerful security compliance management solution. Then, organizations can implement prudent, comprehensive device, database, system, and application security policies and procedures.

With the help of technology, organizations can establish accountability through consistent data collection, retention, monitoring, and reporting practices. Through security compliance management – including proactive risk assessment and management, real-time monitoring and alerting, and on-demand trend reporting – organizations can successfully demonstrate that IT controls support a sound internal control framework that meets security compliance requirements. A risk-based security program begins with a formal risk assessment. The risk assessment must consider historical, real-time, and potential threat events and vulnerabilities to all devices and systems, as well as the underlying internal applications and databases on such devices. The risk-based findings of a formal risk assessment will help identify policies that must be assessed and infrastructures that must be hardened to prevent known and unknown threats from achieving success. If such threat events occur, the organization must take quick, decisive action. Additionally, organizations need to proactively patch any vulnerabilities identified in critical devices, databases, systems, and applications.

An effective Security Compliance Management solution will collect volumes of diverse data and apply sophisticated normalization and aggregation techniques. Multiple correlation technologies, robust visualization, and real-time reporting are required to rapidly identify and document threats. By incorporating an integrated incident resolution workflow, organizations can remediate incidents rapidly and close the loop to ensure compliance and policy refinement.

5

EIGHT ESSENTIAL PRACTICES FOR SUCCESSFUL SECURITY COMPLIANCE MANAGEMENT

Organizations that execute a proactive security compliance management strategy will establish eight key practices to ensure enterprise-wide information security and ongoing compliance. These practices include:

8 ESSENTIAL PRACTICES FOR SUCCESSFUL SECURITY COMPLIANCE MANAGEMENT	
Establish and commit to a policy-driven security management program	Generate security policies that ensure that security controls accomplish their mission. All people, process, and technology controls are instruments of policy, and must implement management intent as stated in a security management policy governing the organization. Security compliance management tools can be configured to implement policy and tie the management of security directly to an organization's policy.
Clearly define the the control environment	Identify the systems, services, devices, data, and personnel associated with the day-to-day use and protection of critical information and systems. When selecting controls, ensure that such controls support the business processes of the organization and its affiliated organizations, such as contractors and industry partners.
Strictly control access	Not only protect the data, but the systems, services, and devices within the organization. Be able to identify which employees, contractors, and partners have physical and logical access to the network, devices, applications, and data for specific and authorized business purposes, and be able to identify and mitigate unauthorized physical and logical access attempts.
Validate security controls	Regularly monitor the environment for performance and effectiveness of the controls in place – including controls on human actions and decisions, process controls, and information technology controls – for successful, measurable risk reduction. Establish baseline activity, study trend-line analysis, and ensure that unusual activity can be quickly identified and addressed, as necessary.
Document all corrective actions	Demonstrate that the proper steps were taken to correct systems and adjust policy if a noncompliant situation is identified.
Study the results of testing and reporting	Continuously manage and oversee the environment through reporting and testing, while providing documented evidence of due diligence to auditors.
Collect and retain data	Take reasonable steps to ensure that sufficient data is collected to identify and respond to incidents and to monitor and enforce policies and service-level agreements. Automated data collection and retention allows organizations to track security and performance indicators across the network and critical applications on a continuous basis, as opposed to periodically – helping to create a proactive risk management process. In addition, a data repository can help organizations leverage security information to learn from the threat environment, improve controls, train employees, and maintain a high level of threat awareness.
Preserve data in its purest form	Preserve near-term and long-term data in its purest form for audit, forensics, and evidentiary presentation.

CYBERSHARK™

CYBERSHARK: SECURITY AND COMPLIANCE PLATFORM SIMPLIFIED

Whether an organization is just beginning to implement solutions for collecting and analyzing log data, enhancing security practices to protect critical data from breaches, or seeking to obtain real-time actionable security and compliance information, BlackStratus can help. BlackStratus Security and Compliance platform continuously manages risk and enables compliance with recognized security best practices by:

- **Collecting and retaining security event data across the enterprise, from the perimeter to the core**
- **Identifying, tracking, analyzing, and remediating both internal and external incidents**
- **Implementing an integrated incident resolution management workflow with embedded knowledge to resolve security incidents**

CYBERShark delivers the most well-engineered security compliance management platform available today: powerful, scalable and flexible. From real-time threat identification and mitigation to log management and audit readiness, CYBERShark is renowned for providing solutions that help organizations take control of security, operations and compliance. CYBERShark platform dramatically improves your organization's ability to identify and rapidly respond to threats. Companies can finally gain an effective, proactive approach to protecting critical data and ensuring compliance with regulatory mandates and corporate policies.

(continued)

CYBERSHARK: SECURITY AND COMPLIANCE PLATFORM SIMPLIFIED

SIM: Size Does Matter

CYBERShark delivers a whole new breadth and depth of security intelligence, regardless of organizational size, type, or budget. Unlike other SIM or Log Management vendors, CYBERShark will not force an overly expensive SIM with more horsepower than you need, or try to ineffectively scale a basic log management solution to fit the needs of a complex, distributed environment. We are the only security and compliance software vendor that has a complete line of solutions to effectively address your specific needs, from both a performance and cost perspective. We believe that no matter how large or small your network, you should not have to make a choice between being secure and being compliant.

Enterprise-Class Security Information Management

CYBERShark transforms huge volumes of disparate, security-related data into understandable, actionable intelligence. Built on a highly-scalable n-tier architecture, CYBERShark enables large organizations with complex networks to centrally gather, analyze, and accurately report on security events and risk posture. By identifying and enabling a rapid response to threats and providing an auditable compliance framework, CYBERShark helps protect valuable data and address a myriad of regulatory challenges.

(continued)

CYBERSHARK™

CYBERSHARK: SECURITY AND COMPLIANCE PLATFORM SIMPLIFIED (CONTINUED)

Flexible, Powerful and Affordable SIM and Log Management Appliances:

CYBERShark– an all-in-one SIM and log management solution – is fast, effective and exceptionally affordable. Easy to deploy and use, its features advanced correlation technologies and real time monitoring for rapidly identifying and prioritizing threats. Add to that comprehensive log collection, documentation and storage - and organizations can now cost-effectively meet compliance demands while enhancing their overall security posture. CYBERShark offers flexible deployment options to accommodate any size networking environment.

Delivering Security Information Management from the Perimeter to the Core Importantly, CYBERShark supports the common security compliance threads by providing organizations a perimeter-to- core set of tools and technologies, including:

Device, database, system, and application monitoring:

Centralized application, system, and device monitoring enables the collection, correlation, analysis, reporting, and retention of audit events from disparate security and network technologies. CYBERShark monitors web and database applications, security and network devices, operating systems, servers, and desktops to identify threats at the network perimeter, as well as malicious and erroneous internal activity. By monitoring and consolidating security activity on all systems, databases, and devices, and by leveraging a highly intuitive security and compliance reporting system, enterprises of all sizes can protect the integrity of critical data – especially from the increasing prevalence of insider threats.

Strong system-wide security event correlation:

CYBERSharks' correlation technologies go beyond simply logging security information by speeding threat identification and providing an accurate picture of risk. These technologies are architected to handle the massive volume of security information from network-related sources, and pinpoint attacks from the inside and beyond based on a thorough understanding of network and user activity. The correlation technologies process large volumes of data from across the enterprise to identify real-time threats and historical patterns. Organizations can leverage this broad security knowledge base and correlate the information to uncover threats that would otherwise go undetected, facilitating proactive security compliance management.

(continued)

CYBERSHARK: SECURITY AND COMPLIANCE PLATFORM SIMPLIFIED (CONTINUED)

Real-time incident detection through visualization and reporting:

With CYBERShark, organizations can visualize threats as well as the security information underlying the threats. Security teams can assimilate information faster and then focus on the real threats, mitigating vulnerabilities before threats proliferate. Through in-depth reporting, key stakeholders and auditors have ready access to actionable information on all security-related issues, such as viruses, worms, and other malicious code, all system status and configuration changes, and privilege and authorization changes.

Compliance dashboards:

CYBERSharks' customizable dashboards provide real-time monitoring and a holistic view of an organization's security posture. And the dashboards also allow security staff to quickly measure threat levels against high-value assets, including those most critical to achieving regulatory compliance.

Incidentresolution management:

By integrating incident response processes with existing corporate workflow systems, CYBERShark enables an accelerated incident response through a best-practice, collaborative approach. Organizations need to continuously reduce risk exposure through timely and effective incident response, even when faced with vast amounts of security data including countless false positives. Using a clearly defined, repeatable, documented security information workflow, organizations can quickly and accurately address security incidents and prove diligence in external and internal audits.

Embedded knowledge base:

CYBERSharks' knowledge base delivers guidance in analyzing, documenting, and reporting on security issues, including newly discovered vulnerabilities, malware, and vendor-specific vulnerability data. Security operators and analysts can obtain a continual flow of relevant and actionable information to pinpoint attacks and provide containment and remediation steps to network and configuration managers. Security teams can get highly specific response guidance in the event of a re- occurrence since the knowledge base can be updated with organization-specific data, including information about a previous incident.

Risk assessment:

CYBERSharks' platform delivers a continuous, comprehensive picture of risk through a suite of risk assessment tools. These techniques and reports capture real- time and historical risk information – pinpointing threats and vulnerabilities at the network and user-activity level. An array of risk assessment reports provides the necessary details behind each technology asset and its associated risk, enabling security teams to pinpoint and prioritize threats. A suite of operational and management reports, available from a customizable dashboard, delivers real-time insight into the risk baseline.

(continued)

CYBERSHARK™

CYBERSHARK: SECURITY AND COMPLIANCE PLATFORM SIMPLIFIED (CONTINUED)

Security operations performance measurement:

CYBERShark gives organizations the tools to measure the performance of security operations, better understand risk, and quantify the success of security compliance initiatives. CYBERShark automates key compliance metrics – from vulnerability metrics to high-level risk metrics – by providing reports that focus on vulnerability, threat, and incident response for all technology assets.

Highly scalable and redundant security architecture –The extensive scalability of CYBERShark architectures cost-effectively support growth and ensure that as an organization grows and changes, its SIM solution can evolve with it. These high-performance architectures also minimize costs by requiring less hardware than traditional SIM solutions. Robust architectures incorporate high volumes of data from across the organization, regardless of the number or devices, applications, systems, and databases. CYBERShark offers the only multi-tier SIM architecture with full failover to help enable reliable, effective security compliance management.

7

CONCLUSION

With security threats evolving, organizations must protect valuable corporate assets by ensuring a strong risk management and security posture. At the same time, they need to maintain compliance with the ever-changing myriad of regulatory mandates and industry standards or face costly consequences. To be proactive, organizations need a practical, cost effective approach to managing security risks while achieving, maintaining, and proving regulatory compliance. Properly implemented, security compliance management dramatically improves security by minimizing threats and reducing risk, making compliance itself much easier to achieve.

By leveraging innovative technologies and tools, organizations can identify, assess, and report on security-related issues and events, and can provide tangible evidence of their efforts. CYBERSharksecurity and compliance platform helps organizations implement strategic, comprehensive policies and procedures for establishing accountability and consistent reporting practices. Through these security compliance management practices, companies can effectively leverage and protect their technology infrastructure while managing enterprise wide information security. Security compliance management can in effect empower companies to accomplish what the regulatory mandates hope to ensure: securing valuable corporate assets and information.

CYBERSHARK™