VULCAN.

Meeting the challenge of risk-based regulatory

01

Introduction
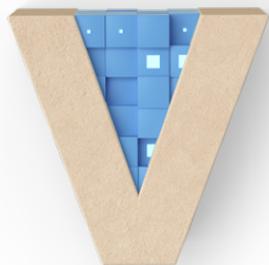
Identifying and analyzing vulnerabilities and their associated risk helps us prioritize and mitigate them. That isn't just critical for good cyber hygiene. It's also a necessary component of many key regulatory requirements and guidelines, such as PCI-DSS, HIPAA, GLBA, GBPR and the NIST Risk Management Framework (RMF). These require organizations in many industries to put in place a vulnerability scanning program that identifies and tracks vulnerabilities - and the actions that have been taken to remediate them. Many of these regulations call for this to be done in a way that consistently and accurately incorporates risk-based prioritization and response.

Vulnerability and cyber risk management are major parts of many key global regulatory requirements and industry guidelines. Some are mandatory, some depend on the industry, and some are voluntary. And while there's a good chance that your business must comply with one or more regulations, effective vulnerability and cyber risk management are regardless critical to securing your organization.

NOT COMPLYING WITH VULNERABILITY STANDARDS CAN LEAD TO A NUMBER OF NEGATIVE IMPACTS:

v **Direct costs of a breach:** Failing to meet vulnerability standards increases the odds of a breach, incurring significant breach-related costs and a loss of revenue.

v **Fines for compliance violations:** Many regulations impose extensive fines for failure to comply, which can grow significantly in the case of an actual incident.

v **Audit stress:** Organizations that fail to comply with regulations are frequently subjected to increased auditing, placing a significant burden on already overextended resources.

v **Reputation damage:** Non-compliance, particularly if it contributes to a breach, can raise significant red flags to customers and partners, damaging your business.

The Vulcan Cyber® risk management platform either directly meets or significantly augments an organization's ability to perform compliance mandated vulnerability management activities for many of the most common industry regulations. Integrations with dozens of vulnerability scanners, asset management platforms, ITIL, communications/collaboration platforms, and many other security solutions allow you to seamlessly orchestrate every step in the vulnerability and risk management lifecycle.

Vulnerability management: Not just a security concern

Regardless of your industry, getting a handle on vulnerabilities and how they impact your overall cyber security posture is necessary to reach an IT maturity level that builds confidence. Being able to answer these three questions demonstrates that your organization can be trusted to handle data in ways that are more secure overall:

Q. DO YOU REALLY UNDERSTAND WHERE YOUR ORGANIZATION IS MOST AT RISK?

Answering this question requires deep analysis of vulnerability, risk severity, asset type, exploitability, threat intelligence, and other types of data to deliver relevant and accurate context to drive your vulnerability and risk management process.

Q. DO YOU KNOW WHAT TO DO ABOUT MITIGATING YOUR CYBER SECURITY RISK?

You need a program in place that will help you remediate vulnerabilities on a timely basis by showing what you need to do and providing the means to do it quickly and consistently, in a way that meets your operating processes.

Q. DO YOU KNOW WHERE YOU SHOULD FOCUS YOUR RISK MITIGATION EFFORTS FIRST?

You need access to threat intelligence to alert you not only to trending vulnerabilities but, most importantly, to vulnerabilities most likely to target your assets.

Vulcan Cyber provides a simple way to address security and regulatory concerns tied to vulnerability and risk management with a single powerful platform.

KEY CHALLENGES

1. Most regulations require vulnerability scanning and patching. But many also expect a level of understanding and plan of action for cyber risk, that vulnerability scanners alone are incapable of delivering.
2. Few organizations have the resources to properly research vulnerabilities for the relevant context necessary to accurately prioritize risk.
3. Many organizations are required to comply with multiple regulations, each with a different set of specific deliverables and reporting guidelines.
4. Documentation of manual processes adds additional time, is often inconsistent, and needs to be done in a way that make reporting on compliance specific activities simple.
5. Keeping up with rapidly changing environments, particularly with cloud infrastructure and application development, makes executing on consistent vulnerability and risk management processes difficult.

03

The Vulcan Cyber solution

Vulcan Cyber is a cyber risk management solution that helps teams meet the challenges of regulatory compliance. Its risk-based prioritization, remediation and orchestration capabilities make it easier for your security, DevOps and IT departments to own their risk.

VULCAN CYBER PROVIDES ADVANCED THREAT INTELLIGENCE THAT LETS YOU...

v Stay ahead of trending vulnerabilities and exploits worldwide.

v Ingest and enrich your data to enable better, faster decision-making.

v Automate vulnerability prioritization and remediation.

Vulcan Cyber goes far beyond compliance-mandated requirements. With better visibility into asset management, risk-based prioritization, and remediation automation and orchestration, along with metrics and reporting for tracking performance, IT and security can become strategic assets for your organization.

HOW VULCAN CYBER HELPS YOUR COMPLIANCE POSTURE:

v Integrates with vulnerability scanners, asset management, threat intelligence platforms and other tools to accurately and intelligently understand and prioritize risk to meet organizational security objectives and compliance specific mandates.

v Analyzes and prioritizes risk based on asset type, threat type and prevalence, logical grouping and any other relevant factor

v Facilitates open communication and collaboration between security, compliance, DevOps, application development and IT operations through out-of-the-box integration with communication platforms, ITIL, etc.

v Allows users to create automated playbooks for collaborating on, responding to, and when appropriate, actively remediating vulnerabilities based on automated risk prioritization. Playbooks can:

» Adapt to any organization's operating processes for opening trouble tickets, communicating priority, presenting the appropriate fix, etc.

» Can be increasingly automated based on organizational comfort levels and need as tasks are more clearly defined.

v Tracks and reports on vulnerability and cyber risk management activities

» Macro and granular risk ratings (security posture) that track program progress and efficacy over time through valuable KPI views.

» Documents what risks/vulnerabilities are identified when, how they can impact the specific organization, and what should be/ was done to respond/remediate.

04
Sample regulations

There are numerous regulations that have explicitly stated
requirements for implementing and reporting on a vulnerability
scanning program. In many cases, this means implementing a strategy
that is based on clearly defined risk and/or deploying a formal
program for executing on and documenting vulnerability remediation.
This section addresses a few of the more common regulations with
vulnerability scanning and risk assessment requirements. References
to specific regulatory requirements are intended to provide common
examples as a starting point for understanding how vulnerability and
risk management can contribute to an organization's compliance.
They do not provide a comprehensive list of required activities and
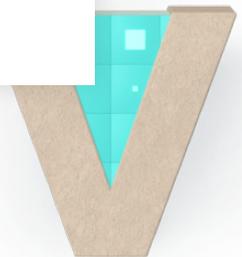
NIST

GOAL:

The U.S. government's National Institute of Standards and Technology (NIST) cyber security frameworks aim to help organizations build resilience against a wide range of threats, including natural

PROTECTS:

Any and all types of sensitive data stored and transmitted by the company: customer information, intellectual property, employee data, and more.

PRINCIPLES:

NIST SP 800-53 (Risk Management Framework), first published in 2005 and updated in 2020, aims to identify and manage cyber security risk through seven steps: Prepare, categorize, select, implement, assess, authorize, and monitor.

EXAMPLES WHERE VULNERABILITY AND CYBER RISK MANAGEMENT APPLIES:

v Implement periodic vulnerability scanning, especially of critical assets **[NIST SP 800-53 RA-5, Control A]**.

v Select tools that enable interoperability and automate vulnerability management **[NIST SP 800-53 RA-5, Control B]**.

v Analyze vulnerability scan reports and results from security control assessments **[NIST SP 800-53 RA-5, Control C]**.

v Remediate legitimate vulnerabilities in accordance with risk assessment results **[NIST SP 800-53 RA-5, Control D]**.

v Share vulnerability and risk assessment information to eliminate similar vulnerabilities **[NIST SP 800-53 RA-5, Control E]**.

Vulcan Cyber can also augment adherence to Controls in RA-1 (Risk Assessment Policy and Procedures) and RA-3 (Risk Assessment) by helping to codify and execute on risk assessment policy implementation.

STATUS:

Mandatory compliance for U.S. government agencies (and potentially contractors and supply

PCI DSS

GOAL:

Developed by five major credit-card companies (Visa, MasterCard, Discover, JCB, and American Express), PCI DSS establishes minimum security standards when storing, processing, and transmitting cardholder data.

PROTECTS:

Cardholder data, primarily primary account number (PAN) in addition to elements such as cardholder name, expiration date, service code (CVV), along with other identifying information.

PRINCIPLES:

The PCI Data Security Standard (DSS), first released in 2004 and updated in 2018, revolves around six goals governing network and information security. Each goal includes highly specific, platform-independent instructions. Audit requirements vary depending on business size; most businesses require self-audit only. Fines range from $5K to $100K per month of non-compliance.

EXAMPLES WHERE VULNERABILITY AND CYBER RISK MANAGEMENT APPLIES:

- v Identify vulnerabilities using reputable outside sources **[PCI DSS Requirement 6.1]**.

- v Protect system components and software from known vulnerabilities and apply critical security patches within one month of release **[PCI DSS Requirement 6.2]**.

- v Address common coding vulnerabilities in software-development processes **[PCI DSS Requirement 6.5]**.

- v Identify all "high risk" vulnerabilities identified in 6.1 **[PCI DSS Requirement 6.5.6]**.

- v Continually address new threats and vulnerabilities for public-facing web applications at least annually and after any change **[PCI DSS Requirement 6.6]**.

- v Perform quarterly vulnerability scans, address vulnerabilities and verify that all "high risk" vulnerabilities are resolved in accordance with risk rankings defined in 6.1 **[PCI DSS Requirement 11.2.1]**.

- v Implement a risk assessment process performed annually and upon significant changes to the environment that identifies critical assets, threats and vulnerabilities and results in a formal, documented analysis of risk **[PCI DSS Requirement 12.2]**.

STATUS:

Mandatory for businesses processing, storing, or transmitting payment card data; some jurisdictions have also incorporated portions of PCI DSS into law.

HIPAA

GOAL:

The Health Insurance Portability and Accountability Act is a U.S. federal statute protecting the creation, storage, and transmission of protected healthcare data.

PROTECTS:

Individually identifiable protected health information (PHI) relating to physical or mental health condition, provision of health care, or payment of health care.

PRINCIPLES:

First signed into law in 2008 and updated in 2013, HIPAA ensures appropriate use of healthcare data and provides patients with access to their own health care data through its Privacy Rule, Security Rule, Transactions Rule, Identifiers Rule, and Enforcement Rule. Enforced by U.S. Office for Civil Rights (OCR). Highest HIPAA fine levied to date is $16M.

EXAMPLES WHERE VULNERABILITY AND CYBER RISK MANAGEMENT APPLIES:

- v Establish safeguards to protect against reasonably anticipated cyber security threats to the integrity of electronic protected health information (ePHI) **[HIPAA Security Rule § 164.306 (a) (2)]**.

- v When deciding which security measures to use, prioritize based on:
    - » The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities **[HIPAA Security Rule § 164.306 (b)(2)(ii)]**.
    - » The probability and criticality of potential risks to ePHI **[HIPAA Security Rule § 164.306 (b)(2)(iv)]**.

- v In accordance with § 164.306, implement policies and procedures to prevent, detect, contain, and correct security violations **[HIPAA Security Rule § 164.308 (a)(1)(i)]**.

- v Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate **[HIPAA Security Rule § 164.308 (a)(1)(2)(A)]**.

- v Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) **[HIPAA Security Rule § 164.308 (a)(1) (i)]**.

STATUS:

Mandatory for certain healthcare organizations operating within the U.S., such as HMOs, and (potentially) subcontractors, partner organizations, and supply chain.

GLBA

GOAL:

U.S. federal law aimed at protecting consumers from financial institutions' misuse of their personal information.

PROTECTS:

Nonpublic personal information (NPI), including names, addresses, phone numbers, banking information, social security numbers (SSN), and more. Information that is fully publicly available, such as address lists, are not protected under GLBA.

PRINCIPLES:

The Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 to ensure that any organization acting as a "financial institution" will safeguard sensitive consumer data and exercise transparency in how that data is shared with nonaffiliated third parties. Fines range from $5K to $1M per day in violation. Specifically, the Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information.

EXAMPLES WHERE VULNERABILITY AND CYBER RISK MANAGEMENT APPLIES:

- **v** The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information.
  - » Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
  - » Design and implement a safeguards program, and regularly monitor and test it.
- **v** The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation.
- **v** Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:
  - » Check with software vendors regularly to get and install patches that resolve software vulnerabilities
  - » Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

STATUS:

Mandatory for organizations providing consumers with financial services such as loans, investment advice, or insurance; includes non-bank businesses that offer loans and financing; potentially also includes certain subcontractors.
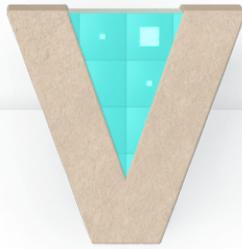
Going beyond:

Vulcan Cyber® breaks down organizational cyber risk into measurable, manageable processes to help security teams go beyond their scan data and actually reduce risk. With powerful prioritization, orchestration and mitigation capabilities, the Vulcan Cyber risk management SaaS platform provides clear solutions to help manage risk effectively. Vulcan enhances teams' existing cyber environments by connecting with all the tools they already use, supporting every stage of the cyber security lifecycle across cloud, IT and application attack surfaces. The unique capability of the Vulcan Cyber platform has garnered Vulcan recognition as a 2019 Gartner Cool Vendor and as a 2020 RSA Conference Innovation Sandbox finalist.

Own your risk.

CONTACT US

VULCAN.