SOLUTION SPOTLIGHT

NAVEX GLOBAL®

Major University with Diverse Requirements Automates Information Security

SOLUTION

LOCKPATH®
INTEGRATED RISK MANAGEMENT

EP NE PT RR LP

HIGHLIGHTS

COMPANY

Major University Division

CHALLENGE

32 depts. have their own IT resources

SOLUTION

Vulnerability Management

RESULTS

100% vulnerability response rate; 77% response time decrease

Information Security with Lockpath

Import, correlate and prioritize results for a contextual view of risks and vulnerabilities

Maintain a complete asset database and conduct periodic IT risk assessments

Manage remediation and escalate risks and vulnerabilities

Create IT risk and security policies and map statements to assets, controls and risks

Manage the incident lifecycle, from root cause analysis to corrective action plans

Create role-based interactive reports and tailor messaging to different audiences

Challenge: Decentralized Structure & Open Culture Challenge Information Security

A major university's biosciences division included 5,000 faculty and staff spread across 32 departments, each with its own IT support and unique cybersecurity requirements. These departmental silos prevented the security team from assessing the entire IT landscape. It also created gaps in security controls, inconsistencies with applying security controls and duplication of efforts.

Another challenge for information security was the university's commitment to open inquiry and interdisciplinary research. From an information security perspective, freely sharing information throughout the university, with other institutions and around the world introduces risk.

For the security team, the last straw was trying to follow the Federal Information Security Management Act (FISMA) procedures and controls for protecting government information, operations and assets against threats. The only way for the university division to meet FISMA requirements was to add headcount (a nonstarter) or seek a technology solution.

Solution: NAVEX Global's GRC platform, Lockpath

The university division selected NAVEX Global's governance, risk management, compliance (GRC) platform, Lockpath, for its capabilities in integrated risk management (IRM). Lockpath enables the university to gain a comprehensive view of their business and operations from a risk perspective—connecting individual risk disciplines and managing them in one centralized program.

Before getting up and running with Lockpath, the security team completed some groundwork. It entailed process mapping, defining roles and responsibilities, classifying and taking inventory of information systems, as well as defining a process for automating cybersecurity tasks like scanning, prioritizing, assessing and reporting vulnerabilities. Assets were given a confidentiality, integrity and availability (CIA) score to determine its importance to the division's operations.

The security team entered all data and new processes into Lockpath for recordkeeping and asset monitoring. Lockpath automatically performed a Priority Impact Analysis (PIA) on each new vulnerability detected across the IT landscape of 32 departments. The team consulted a heat map on a dashboard showing the PIA score, along with the asset CIA score. As a result, the team could address the most severe vulnerabilities first and manage the entire process more efficiently. Conducting activities in Lockpath also made it easier to comply with FISMA Moderate procedures and controls.

LOCKPATH®
Integrated Risk Management

Integrated Risk Management

Integrated Risk Management (IRM) is the collection of practices and processes that offer a comprehensive way to identify, assess and prioritize risk throughout an organization. Lockpath, a GRC and Integrated Risk Management solution from NAVEX Global, equips users and business leaders to manage risk from the endpoint to the enterprise.

Lockpath's integrated risk management capabilities address eight business use cases:

- Compliance and policy management
- Vendor risk management
- IT risk management
- Continuous monitoring
- Business continuity management
- Operational risk management
- Audit management
- Health and safety management

The division's 32 departments were involved in managing vulnerabilities as well. After a scanner detected a vulnerability and sent details to Lockpath for processing, the solution automatically notified the IT custodian and sent reminders until the vulnerability was addressed or escalated to the appropriate party. For vulnerabilities addressed but not remediated, a root cause analysis was performed, and a mitigation plan was implemented.

Results: A Streamlined Approach to Managing Vulnerabilities with Cross-Department Buy-In

The security team's unified approach to vulnerability management was accepted by all 32 departments. Response time to address vulnerabilities was reduced by 77%, while automating scanning and processing activities promoted accountability among departments. As proof, 100% of vulnerabilities were addressed.

Key to the 100% success rate was automating notifications and reminders. Automated messages compelled IT custodians to take action to stop notification and prevent escalation. In addition, whether it was the IT custodian, system owner or department head, individual dashboards reported only information that was applicable to each role. Stakeholders were empowered and accountable in managing vulnerabilities and remediation activities.

The division's program transformed the IT security team. Despite the challenges of a decentralized IT structure and the university's open culture, Lockpath automated vulnerability management, making it accurate, accepted and accountable.

ABOUT NAVEX GLOBAL

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services. Trusted by more than 14,500 customers, our solutions help organizations manage risk, address complex regulatory compliance requirements and foster an ethical, highly productive workplace culture. For more information, visit www.navexglobal.com.

© 2020 NAVEX GLOBAL, INC. ALL RIGHTS RESERVED. | 06.11.20