FORTRA

CASE STUDY (DIGITAL DEFENSE)

Digital Defense Helps Investors Bank Enhance Their Information Security Posture

The financial services and banking industries are some of the most highly regulated institutions in the world. Security breaches continue to wreak havoc on businesses and stay in the headlines.

With the exponential growth of digitalization, including online banking, these organizations hold a tremendous amount of personal data and therefore protect more than just digital facts and figures – they protect the confidentiality of data, and therefore the future quality of people's lives. It is a big undertaking. How these businesses handle or mishandle data can make all the difference in the world to the data owner.

There are organizations that take compliance one step further. These institutions focus on creating a culture of not only compliance but also resilient security to protect their customers, employees and partners. This can seem like a daunting task with hackers innovating faster than many organizations can keep up with, but it should be the goal of every organization to make whatever improvements possible to protect its most valuable assets, its people.

The Challenge

Though compliance regulations have driven security efforts in previous years, these regulations cannot always stay ahead of the quickly moving threats that continue to emerge. Investors Bank understands the importance of maintaining topnotch security by protecting the organization and its customers from all points of intrusion, from their employees to their network infrastructure.

Investors Bank has always embraced security best practices but they were savvy enough to know they needed to increase security to stay ahead of evolving threats.

Some challenges the institution faced were:

- Managing the vast amount of associated security data
- Understanding the highest levels of risk to ensure remediation efforts were targeted and focused
- Effectively communicating complex technical information on the Bank's security posture

AT-A-GLANCE

investorsBank

About Investors Bank

focus on a multipronged approach to ensure a robust and resilient security posture. With the management of financial assets and personal data comes great responsibility and organiza-tions such as Investors Bank take this responsibility very seriously.

Investors Bank was founded in 1926. They are now one of the largest banks in the New Jersey and New York areas, with over 145 branches, and Investors Bancorp, Inc. is publicly traded on NASDAQ.

Investors Bank has a strong mission and vision that are built on four core values:

1. Cooperation: The act of working together toward a common purpose or benefit
2. Character: The combination of features and traits that form the individual nature of a person or team
3. Community: A self-organized network of people who collaborate by sharing ideas and information for the sake of the common good of the organization, community and customers
4. Commitment: A pledge, promise or obligation to their customers, community, employees and partners

The Goals

Investors Bank didn't get to this solid security strategy and posture overnight, and they knew it would be a marathon, not a sprint, to cover all points where they may be susceptible to an attack – such as implementing employee security awareness training or leveraging proactive vulnerability management technology.

Important to the team was to not only verbalize the Investors Bank values but to also adhere to their vision by taking action and innovating. They wanted to implement strategy risk, control and defense in depth. Damiano Tulipani, Vice President, Cybersecurity Manager, joined the Information Security Department at Investors Bank in March of 2017 to help enhance the Bank's information security program.

Joining Tulipani shortly thereafter was Information Security Analyst, Joseph Li, an experienced cyber professional. The information security program and strategy was reinvigorated, with a key objective that all internal and external stakeholders become active participants in the journey towards impeccable cybersecurity practices.

The following goals were established:

- Facilitate a "One-Team" security culture in which all employees are invested in being the front line of defense against cybercrime
- Provide information security training to new hires
- Responsible for managing security awareness campaigns throughout the year including but not limiting to security newsletters
- Demonstrate leadership and commitment to security best practices through participation in the National Cybersecurity Awareness Month (NCSAM) with the dissemination of weekly email campaigns to employees and customers
- Commit to educating customers about information security to ensure they are personally protected and do not introduce risk to themselves
- Conduct community outreach to educate, such as presenting to the American Bar Association (ABA) on information security best practices
- Protect data by leveraging top notch technologies and cybersecurity risk solutions
- Identify and manage vulnerabilities proactively to detect the highest areas of risk, enabling rapid remediation

Investors Bank requisites for information technology encompassed a vulnerability management system to:

- Manage and balance network risk to an acceptable level, and focus on the remediation of critical, high and medium vulnerabilities
- Optimize resources through automation and establish Key Risk Indicators (KRIs) to manage risk
- Quickly identify and prioritize vulnerabilities to assist in accomplishing the internal standard remediation time for asset owners of 30 days for critical and 60 days for high vulnerabilities
- Provide metrics to communicate progress and the bank's dynamic information security posture to key Investors Bank stakeholders including executive staff and the Board

Digital Defense's Role in Investors Bank's Security Program

According to Joseph Li, Information Security Analyst at Investors Bank, Frontline VM aids in strengthening the vulnerability management strategy because it streamlines the information security program through:

- *An easy to implement and manage system*
- *The elimination of extensive research required to determine how to resolve vulnerability issues*
- *Tracking and trending features to help manage risk*
- *Excellent support and service*

The Solution

Investors Bank evaluated all security technologies to ensure they were equipped with the strongest solutions to deliver the highest level of information security. Through this evaluation, the team determined Frontline Vulnerability Manager™ (Frontline VM™), a Frontline.Cloud system long utilized by the institution, remained the preferred solution.

"Investors Bank has been using Digital Defense for 9 years now and by utilizing the unique Frontline Security GPA® feature within their Frontline.Cloud platform we've been able to improve our internal and external grade from a C - to an A -. Investors Bank has realized a positive change in a short period of time by building out an innovative information security strategy and lever- aging Digital Defense tech- nology. The work conducted over the past year has resulted in a level of acceptable risk which is viewed favorably by auditors and the FDIC."

- Damiano Tulipani, Vice President, Cybersecurity Manager for Investors Bank

Investors Bank has illustrated industry recognized work in security, and even received Digital Defense's 2017 Excellence in Network Security Award for one of the highest Frontline Security GPAs within the Digital Defense client community. Their security awareness focus contributed to Investors Bank receiving the National Cybersecurity Awareness Month (NCSAM) Champion award for promoting cyber awareness to their internal and external customers.

Technology Spotlight

Frontline VM is a comprehensive, accurate, user-friendly vulnerability management software, industry recognized for accuracy and ease of use.

Features include:

- Lightweight, agentless scanning that minimizes network and endpoint footprint
- Patented endpoint scanning correlation technology that eliminates "network drift"
- Dynamic dashboard, data analysis and reconciliation
- Automated asset classification, risk prioritization and remediation assignment
- Concise, actionable intelligence with step by step instructions on how to quickly fix vulnerabilities
- Authorized user access from any location
- Customized user permissions and rules
- Workflow management with assignment tracking system
- Trending and labeling notifications, highlighting unmitigated vulnerabilities and new asset discoveries
- Frontline Security GPA® – unique rating system that provides a clear, easy-to-understand picture of an organization's security posture

Contact us: Sales@digitaldefense.com

For more information visit: www.DigitalDefense.com

At the time of this case study, Fortra VM and its corresponding security solutions were referred to under the Frontline brand.

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

Copyright © Fortra, LLC and its group of companies. Fortra™, the Fortra™ logos, and other identified marks are proprietary trademarks of Fortra, LLC.