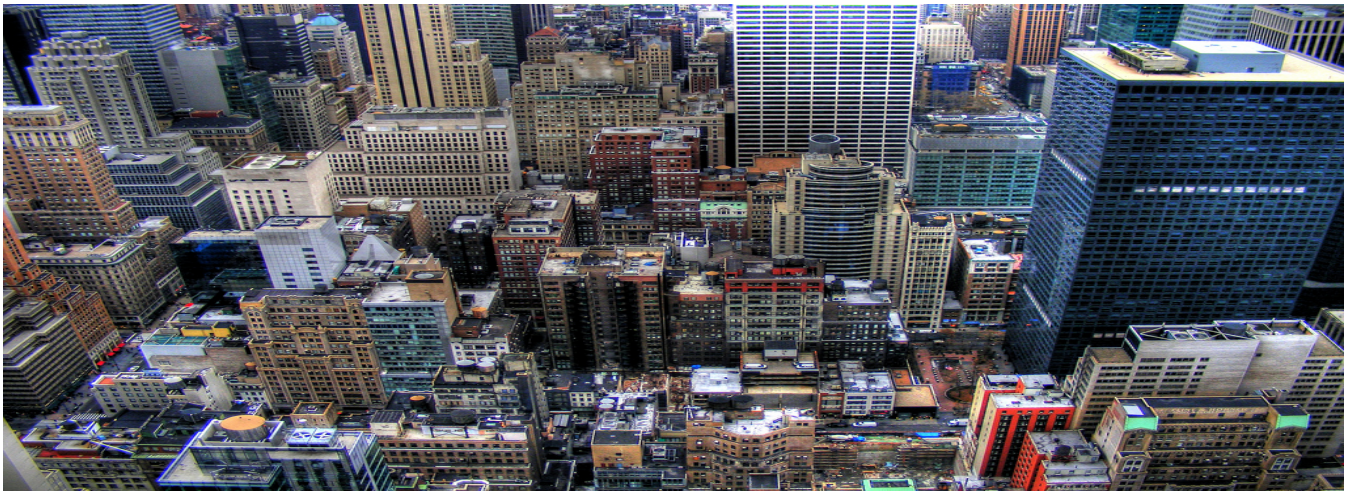
## Aligning business processes with new regulations

Large Insurance Company

# COMPLYING TO 23 NYCRR 500



### CUSTOMER PROFILE

As a leading Insurance provider in the Northeast, writing over $1 Billion in annual insurance premiums and managing more than 550 Million in statutory equity.

### CHALLENGES:

- ✓Comply with 23 NYCRR 500 which went into effect on March 1, 2017.
- ✓Adhere to strict deadlines as defined.
- ✓Protect customer information as well as the technology systems.
- ✓Create a framework to meet/exceed the stringent regulations.

### RESULTS:

- ✓Conduct in-depth Vulnerability assessment and Network Forensics analysis.
- ✓Create a repeatable framework.
- ✓Define 23 NYCRR 500 regulatory reporting Processes.

## THE PROBLEM

The Insurance Company was required by regulation to adhere to **NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES 23 NYCRR 500** which took effect on March 1, 2017. This regulation had specific and detailed timelines for achieving targeted goals. The stringent regulations were designed to promote the protection of customer information and the information technology systems of regulated entities.

Under this new regulation, the insurance company was required to comply or face severe penalties. If a security breach were to occur, the damage could potentially be devastating. In addition to the costs associated with business interruption, reconfiguring damaged machines and funds lost due to theft. Any security breach could also mean lost trust between the Insurance provider and its customers.

The customer was concerned about aligning with these new regulations and creating a repeatable, process to maintain the strength of its network security. In addition, the Insurance company required a continuous testing and monitoring of the cybersecurity program that would provide insight into potential vulnerabilities, how to remediate, as well as support the identification of security program improvements.

## SCOPE & CRITERIA

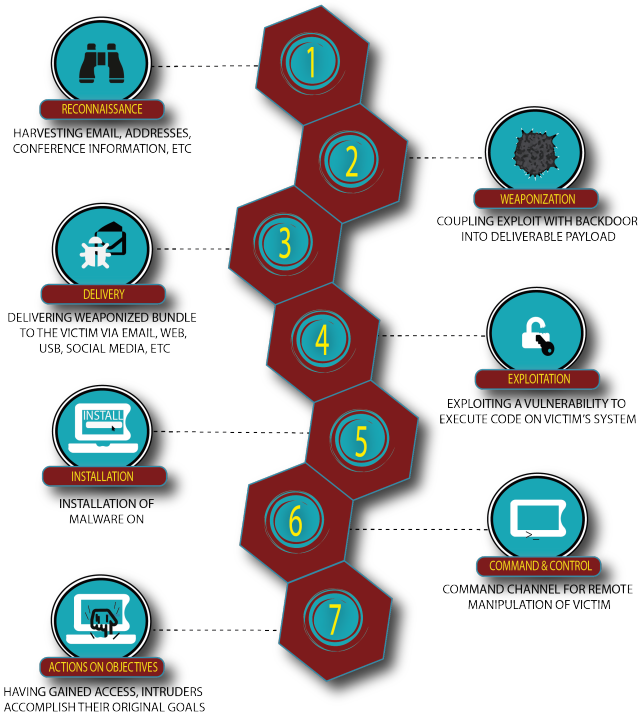
The stakes were high for the customer's IT Security and Legal Teams. The project consisted of 4 phases which included:

- In-depth assessment of the organization's cyber security vulnerabilities and network forensics
- Design an audit framework
- Audit NYS Cybersecurity requirements
- Perform a Cyber Risk assessment

## ENGAGEMENT

iPRESIDIUM performed a vulnerability assessment of the organization's internet accessible systems. Key steps involved system identification and vulnerability scanning. In addition, we conducted a network forensic scan and an email campaign to evaluate security awareness against social engineering attacks and any unauthorized activity on the network.

With Network Forensics, we simulated Advance Persistent Threats (APT) and Ransomware by leveraging Cyber Security Threat Monitoring Services to detect, analyze and respond to stealthier attacks in real-time. Our solution provided the ability to monitor all network ports and protocols along with custom sandboxing to identify command-and-control (C&C) communications, and/or other evasive techniques. iPRESIDIUM provided 60 days of full monitoring and remote management of monitoring and anomalous detection.



## THE SOLUTION

The entire project took 6 months to complete providing the Insurance company with the comprehensive evaluation of their current Cyber Security practices in comparison to the New York State regulatory requirements. The Cyber Risk assessment delivered a transition road-map to compliance, and the Insurance company with the ability to self-update the compliance audit on an annual basis.

Following iPRESIDIUM'S engagement, the Insurance company quickly realized a number of benefits from the 23 NYCRR500 regulation and their security risk management processes:

- An auditable framework designed to provide visibility across the entire enterprise.
- The ability to easily and quickly align with the 23 NYCRR 500 regulations.
- Strengthen control and prioritize risk in the network.

Our client is now able to keep management up-to-speed on their security posture and compliance, while providing intelligence for fast and informed security decisions.

# About iPRESIDIUM

iPRESIDIUM is a cyber security and risk advisory firm. We provide end-to-end enterprise security services for private and public entities of all sizes. iPRESIDIUM helps customers protect their business, employees, data, and their reputations. We succeed by offering our clients cutting edge technologies with best-in-class security solutions, experienced industry professionals proficient in cyber security and managed service platforms. Our goal, to deliver our clients' the peace of mind they need so that they can focus on their business.

Since its inception in 2002, iPRESIDIUM has successfully exceeded the security needs of numerous organizations, across the following sectors: Healthcare, Retail, Education, Government and Public Sector, Financial, Technology, Hospitality, Insurance, Transportation and Manufacturing as well as over 50 US federal agencies and the intelligence communities.

www.ipresidium.com | info@ipresidium.com | 949-721-6612