

Cybersecurity Overview

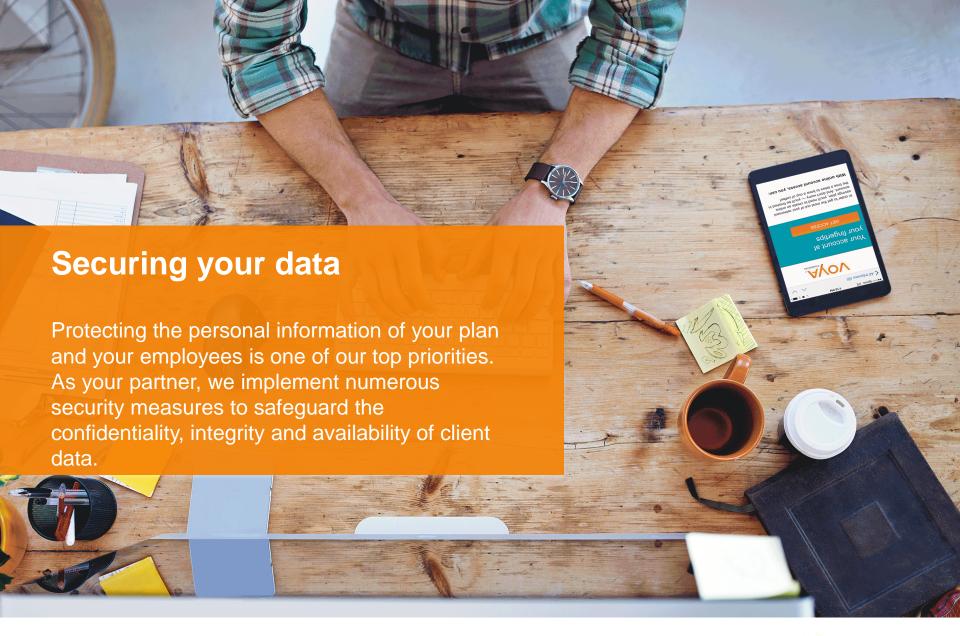
December 5, 2017



Information contained herein is proprietary, confidential and non-public and is not for public release.

PLAN | INVEST | PROTECT







Evolution of the threat landscape

Sep 2017 Jan 2015 Equifax Anthem · Over 140 million users' personal · 80 million member PII compromised information compromised. · Targeted phishing tactics obtained · Exposed information included PII, privileged access PCI and credit history. Nov 2013 Despite database encryption, · Hack leveraged web Struts unauthorized access occurred vulnerability. **Target** Estimated losses \$100M+ Estimated losses > \$325M Sep 2016 Jan 2007 Hackers installed malware on POS 40 Million credit & debit card numbers Yahoo! TJ MAXX Mar 1999 Card information sold on black market Loss estimates in excess of \$300M · Two separate incidents 500 Million Melissa 45 million credit card records Microsoft then 1 Billion user emails accounts Virus compromised Outlook Account info may include PII along Nov 2014 Malware stolen over 18 month period with security questions Customer PII stolen because of · Discovered when user info was Email which contained Word macro unmasked stored data being sold online **Sony Pictures** Self-spreading: emails itself to random Estimated losses \$162M+ Estimated losses \$1B+??? 50 people from address book · Forced Intel, Microsoft & Lockheed Value of damages \$80M · Leak of SSN of employees & Jan 2009 celebrities Leak of embarrassing emails Prompted Co-Chair resignation Heartland Feb 2000 nherent Risk Restoration Costs \$125M+ Nov 1988 MAFIABOY 130 million credit card record Web Vulnerabilities · Hackers compromised external web NETECTED ! Morris Worm systems to gain access Social Engineering Once inside, sophisticated Malware · Youth hacker launched Denial of was deployed to "listen" to network **Banking Malware** Service attack · Designed to spread on Unix systems Estimated losses \$140M+ Crippled major websites: Yahoo, eBay. · Propagated itself using network Key Logger, Bitcoin, CNN, E*Trade, Amazon Infected 6,000 computers in short Denial of Service. · Prompted White House Cyber Summit Identity Theft, Fraud period of time Estimate \$1.2B damages Malicious Emails. · Slowed down the internet Phone Hijacking, Ransomware, Value of damages \$80M Ransomware. "Point of Sale" Attacks. "Point of Sale" Cyber Warfare **Phishing** Attacks 1997 1988 2004 2007 2010 2013 2016 PLAN | INVEST | PROTECT

People, technology & process to protect client data

PEOPLE

Highly skilled security professionals with a robust security awareness program for the entire Voya workforce



TECHNOLOGY

Layers of security controls to provide maximum protection with proactive threat intelligence collaboration across the industry, government agencies, and security firms

PROCESS

Industry best practice controls and processes to ensure your data is secure



Our people

Highly skilled and continuously improving

Conduct monthly phishing tests across Voya Financial™ monthly

85,000 individual phishing tests annually to train employees on how to avoid phishing attacks.

- Dedicated and certified information security professionals
- Participate in global ethical hacking competitions.
- Trained front line employees as the first line of defense on fraud detection and prevention



Our technology

Protecting your data starts from within

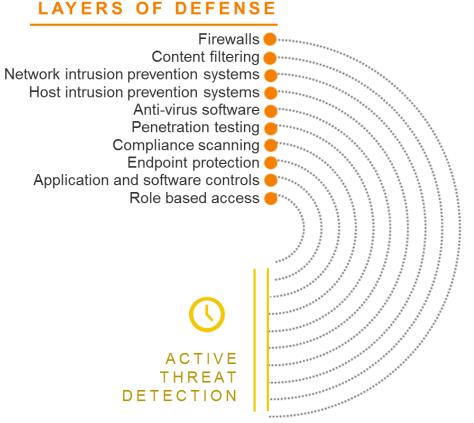
Layers of security controls working in unison to provide stronger protection, to client data

- Automated notification of threat intelligence
- Robust identity verification
- Leverage predictive modeling
- Independent third-party testing



Our technology - protecting data starts from within

Designed to prevent corruption of data, block unknown or unauthorized access to our systems and safeguard client data



EXTERNAL & INTERNAL THREATS

Inappropriate access
Exfiltration of data
Physical security
Unauthorized access
Hacking
Vulnerabilities
Viruses
Third party access
Malware
Phishing



Our process

Industry best practice controls

Industry best practice

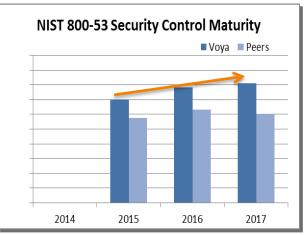
policies and controls as evidenced by SOC 1 and SOC 2 certifications.

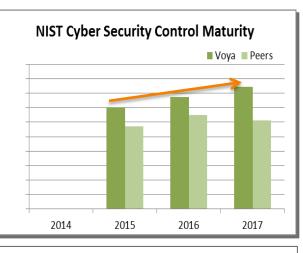
- Department of Homeland Security provides us with information on domestic and international threats, which we incorporate into our security protocols.
- Part of a government-sponsored organization that helps us stay informed of security risks
- Compliance to SPARK data security best practice standards
- Peer benchmarking results show that Voya is well aligned and slightly ahead of peers with respect to policies and supporting controls alignment to ISO and NIST standards



Our Process – Improving Year-Over-Year







Information security management to protect the:

- Confidentiality
- Integrity
- Availability of customer and company information

Security and privacy control requirements for information systems that are used by organizations that support federal entities

Building on the NIST 800.53 standards for:

- Access controls
- Security functions
- Internet security

Note: Current CEB/Gartner benchmarks Voya against companies from Financial Services, Insurance, High Tech, Manufacturing, and Retail industries.



Our process - in the event of a cybersecurity incident

Voya's highly-specialized security incident response team (SIRT) trained to manage cybersecurity related incidents





Q&A

