



# **What Are You Doing to Protect Member Data**

# Protecting Member Data

While no organization can ever be 100% safe from cyber attacks, basic “**blocking and tackling**” security protocols should be in place in all organizations.

Multiple, duplicate “layers of protection” are needed to protect all points of entry and devices on your local area network.

## Firewall

- Need a good “rules based” appliance monitoring traffic and restricting incoming web traffic to specific ports.
- Should offer intrusion detection and prevention features.
- Can offer first level screening for crimeware.
- Can offer ability to send text messages to technology staff cell phones for high threat activity.
- Consider installing a secondary firewall of a different type/brand than your primary one, for redundancy. The secondary firewall should offer artificial intelligence to detect potential harmful activity from internal and external sources.

## Network Switches

- Should offer intrusion detection and prevention features, having the ability to automatically shut down a port showing “unusual or threatening” activity.

## Security Logs

- Install third party software that records and archives security logs for “high profile” (your pension administration solution) servers.
- These logs need to be manually reviewed daily by your security personnel for “suspicious” activity.

## Server and Desktop Protection

- Install a good third party crimeware detection solution on desktops and servers. Even though your firewall screens for crimeware, for redundancy, a solution offering a “deep scan” feature should be installed on desktops and servers.
- Automatic signature updates should automatically be pushed to the desktops and servers at least twice daily and automatic twice daily scans of servers and desktops should be done.
- Consider eliminating CD drives and disk drives from the desktops of users without a business need for them.

## Email Screening

- Although server and desktop protection solutions, and firewalls, can screen email for crimeware, for redundancy and more granular screening of email for crimeware, install a third party email screening application.

## User Authentication

- To protect against password cracking software, password phishing attempts by external entities, and simply carelessness by users in protecting their network passwords, consider using “security tokens” that generate unique numerical passwords each minute.
- RSA SecurID is an excellent two-factor user authentication system. To gain entry to your network, the user must have the security token and a unique PIN.
- Use the security tokens for access internally and externally to your network.
- For users who have no need to access your network at nights or on weekends, use network policies to limit their access to certain hours and/or days.

## **Remote Connectivity to your Network**

- Always use security tokens for authentication of remote users.
- Your chosen solution for remote access should encrypt (128 bit minimum) all traffic to and from your remote user.

## Web Traffic from Internet Browse

(Within your Organization)

- Use a web filtering product to transparently monitor report on, and manage employee use of the internet. This product will also scan web traffic for crimeware, as a secondary backup scan to your firewall.

## Web Traffic to your Web Servers

**(Customers accessing their accounts via the web)**

- Your firewall's "demilitarized zone" should offer partial protection of your web server, but because of the web server's purpose it cannot be fully deployed behind your firewall.
- But, your web application server should be located securely behind your firewall.
- Communication between the web server and web application server should be highly restricted by application code and rigid firewall rules.
- Customer traffic from the Internet to your web servers should be encrypted using Secure Socket Layer (SSL).
- Communication between your web application server and your pension administration solution should also be highly restricted.

## Independent Security Audit

- At least twice yearly it is prudent to have an independent network security firm conduct an intrusion and penetration test of your network.
- The firm will use sophisticated hacking techniques to test the security of your network defenses.

**In Closing...**

***GOOD LUCK!!!***