LAYERED SECURITY

Network security can be strengthened by architecting it into multiple layers, each one often taking a different approach than those adjacent. One such method of layered security calls for multiple vendors to do the same job, one after the other in succession, from the outside world into the protected corporate environment. In other words, the chain is no longer only as strong as the weakest link; now an attacker must break all of the links.

15 Ways To Keep Your Information Secure

1. Use two-step authentication wherever possible. Visit turnon2fa.com to find step by step instructions for any site.
2. Create strong passwords with a combination of letters and numbers.
3. Be careful what information you share on social media.
4. Keep all software up to date.
5. When shopping online, choose https sites.
6. Physically secure laptops and mobile devices at all times.
7. Don't click on unknown links or open suspicious attachments.
8. Do not use public computers for sensitive information.
9. Be cautious of unknown flash drives.
10. Be cautious when using wireless networks; use VPN connectivity when accessing sensitive data.
11. Don't fall victim to "your computer is infected" messages or messages making unrealistic threats or demands.
12. Use encryption for all sensitive data on computers and removable media.
13. Password protect all computers and smart-phones, and keep your username/password safe.
14. Back up your data regularly.
15. Ensure all your PCs use antivirus software.

RAYMOND JAMES®

INTERNATIONAL HEADQUARTERS:
THE RAYMOND JAMES FINANCIAL CENTER

880 CARILLON PARKWAY
ST. PETERSBURG, FL 33716
800.248.8863

RAYMONDJAMES.COM

KEEPING YOUR INFORMATION SAFE

Raymond James safeguards your information with advanced security infrastructure, applications and personnel.

RAYMOND JAMES

Raymond James takes the security of your information seriously. To protect the data we work with from constant threats and attack, the Information Security team uses advanced infrastructure, applications and personnel.

BEST-OF-BREED SECURITY PRACTICES

Keeping all of our clients secure against thousands of attacks each day requires diligence. Here are a few of the ways we keep you safe:

NEXT-GENERATION FIREWALLS

Firewalls block unwanted incoming internet traffic, stop users from downloading and installing viruses, and prevent users from connecting to malicious or harmful websites.

INTRUSION-DETECTION SYSTEMS

Every day, there are thousands of failed attempts to compromise our networks. Information Security logs them through the use of advanced Intrusion Detection Systems. These systems alert Information Security when attempts are being made on a network and allow the team to quickly respond to possible threats.

DATA-LOSS PREVENTION

Human error, miss-clicking, a misunderstanding of policies or malicious intent can all lead to users attempting to move sensitive data outside our networks. Data Loss Prevention (DLP) software stops this from happening. DLP software looks for sensitive data that is being used incorrectly when it is being worked on by a user, transferred through our networks and systems (email or file transfer), or stored incorrectly.

SECURITY INFORMATION AND EVENT MANAGEMENT

Security Information and Event Management (SIEM) software provides quick analysis and management of the millions of security event logs that are generated every day. SIEM allows Information Security to quickly sort through false positives and focus its efforts on correlating interrelated attacks and combating real threats.

EMAIL SECURITY

Email is one of the most important tools employees at Raymond James use every day. We transmit important information through email all day and rely on it to get our jobs done. Threat actors use email to attack our employees and networks. Raymond James stops these attacks by filtering emails to remove and stop emails that have malicious links, attachments, or are simply spam.

LAPTOP AND DESKTOP SECURITY

The laptops and desktops we work on every day need to be protected from a wide variety of threats both inside and outside of our networks. Information Security protects the vital information stored on this equipment by enabling advanced encryption, security and anti-virus software on all Raymond James equipment.

NETWORK AND APPLICATION VULNERABILITY SCANS

The thousands of applications that run on our networks need to be constantly watched for new vulnerabilities. To accomplish that, Information Security runs constant network and application scans. As attackers discover and even create new ways to access systems and hack applications, Information Security stays one step ahead by constantly scanning all of our systems for possible vulnerabilities.

PENETRATION TESTING

Penetration testing, or pentests, as they are often called, is sometimes portrayed as light-hearted IT war games; however, they are anything but that. Real-life pentests must be carefully conducted to determine the potential impacts of a successful attack, while avoiding any actual network or application outages. Pentesting checks our networks for common loopholes and security exploits to ensure protection against common threats.

NETWORK ACCESS CONTROL

Because today's technology standards make it easy to connect just about any device to the corporate network, great care must be taken to ensure only qualified devices are permitted to do so. Without Network Access Control (NAC), an attacker could easily connect to our network and begin to infiltrate sensitive systems. In addition to preventing attackers from connecting devices, NAC can disconnect otherwise authorized devices that have become infected with a virus or otherwise compromised.

TWO-FACTOR AUTHENTICATION

All passwords have one common weakness. Once the password becomes known to others, it is useless. By incorporating an additional factor, this weakness is alleviated and security is strengthened. Security tokens, security questions or thumbprints are all means of providing this additional security.

MOBILE DEVICE SECURITY

Mobile devices are a modern convenience in everyday life. However, without careful consideration toward what those apps are doing, control of the mobile device could be lost to malicious attackers. Through Mobile Device Management, the applications and access of the mobile devices that connect to our corporate network can be subjected to strict controls that permit normal, legitimate activity, while preventing unauthorized access.

DEDICATED THREAT INTELLIGENCE TEAMS

As the theft of both corporate and personal data has become lucrative, this crime has become quite organized. Today, teams of hackers work together to steal sensitive data. To combat this, those responsible for the security of this data must also team up. Raymond James employs teams dedicated to threat intelligence made up of positions and responsibilities that include information gathering, research and testing.