EzeCastle
INTEGRATION

Critical Cybersecurity Threats & How to Prepare in 2014

industry advice and best practices for hedge funds and investment firms

About Eze Castle Integration
Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 650 alternative investment firms worldwide, including more than 100 firms with $1 billion or more in assets under management. The company's products and services include Private Cloud Services, Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford. Visit us at www.eci.com.

Table of Contents

The Industry Today……………………………………..…………………………………………………….…...... 3

Highlights from SEC Cybersecurity Roundtable.. 4

A Hacker's Toolkit: Cybersecurity Threats to Financial Firms ………………………………………….. 5

Best Practices: Building a Secure Investment Firm …………………………………………………………. 8

A Few More Best Practices …………………………………………………………………………………………… 10

Cybersecurity Incident Response: What Now? ……………………………………………………….…. 11

Don't Forget About Mobile Security ………………………………………………………………………….. 12

Conclusion ……… 13

About Eze Castle Integration ………………………………………………………………...………………….. 14

THE INDUSTRY TODAY

The financial services industry has undergone a series of significant changes in recent years. Post-Madoff and 2008 economic crisis, we've seen the proposal and implementation of new regulations, a surge in investor due diligence requirements and a constantly challenging marketplace that has led to a transformation in the way funds do business.

Perhaps of greatest significance is the focus on cybersecurity – as a result of a number of high-profile security breaches and vulnerabilities and an impactful "hacktivist" community looking to leave their mark on the world. The financial services industry, in particular, remains a target of cyber-attacks, and while engaged in an arms race as security threats constantly evolve, hedge funds and their investors continue to advance security postures to mitigate risks.

The threat landscape changes on a daily basis and requires firms to stay diligent and proactive in maintaining security programs that not only protect from external attacks but also from more likely internal breaches. Though not always intentional, internal security incidents are far more likely to occur and cause damage to a firm's operational infrastructure. In other cases, security bugs arise that threaten to destroy countless businesses. Just this week, an Internet bug known as Heartbleed was discovered after a flaw was noticed in code designed to keep servers secure. And not just the servers at one particular firm or retail chain. This particular bug was discovered on OpenSSL, an encryption software believed to be found on up to 500,000 servers.

Regardless of the method or root location, these security threats are real, and the only true way to thwart an incident is to establish a layered security program to safeguard against attacks and vulnerabilities of all kinds.

This whitepaper serves as a guide to hedge funds and investment firms looking for the latest information on cybersecurity threats to the industry as well as offers practical advice on building and maintaining a secure operational infrastructure and ongoing security program. We'll share the outcome of the Securities and Exchange Commission's (SEC) recent roundtable on cybersecurity as well as provide guidance on how to respond to a security incident if and when it does occur.

HIGHLIGHTS FROM SEC CYBERSECURITY ROUNDTABLE

In a move to stress the importance of the topic, the SEC held a lengthy roundtable in March 2014 with the sole focus on cybersecurity. In her opening statement, SEC Chairwoman Mary Jo White stated that cybersecurity is a global concern and first on the list of the Division of Intelligence's threats, surpassing even terrorism. With a host of critical areas susceptible to attacks, finance remains the top target, meaning investment firms must get ahead of such threats in order to mitigate risks.

The good news is the financial services industry tends to employ more advanced security programs than other sectors. That said, now is the time to reevaluate those programs and shore up operations to prevent any imminent threats from a security perspective. According to experts on the roundtable, running simulations and test exercises is the best method to staying a step ahead and detecting risks quickly.

The roundtable stressed that operational risk is the number one threat to financial services firms. This risk can be found in two primary areas – insider risk and IT failures. Insider risk encompasses any actions (whether intentional or unintentional) taken by employees in which they threaten or damage the company's security integrity. This could mean something as simple as loading sensitive information onto an external hard drive or downloading data onto a personal email account. IT failures, on the other hand, cannot generally be attributed to specific internal personnel, but rather are the result of infrastructure threats that leave the company subject to external attack such as malware, phishing attacks and hacker penetration.

At a high level, the SEC advised firms to ask three critical questions during the preparedness stage:

1. **What should be protected?** Multiple layers of security should be employed to protect all systems and data as appropriate. These include, but are not limited to, anti-virus and anti-spam software, host-based and network intrusion detection systems, hardware and software firewalls, encryption tools and application filters.

2. **How do you manage access for insiders and third-party vendors?** Start by implementing and enforcing an Access Control Policy to manage which internal and external parties have access to what data and applications. As a next step, employ a host-based intrusion detection/prevention system which can identify anomalous behavior, such as process injection, keystroke logging, driver loading and call hooking.

3. How do you monitor the monitors? Employ a central logging system that records all login/logout events, as well as inbound/outbound connections through Internet-facing firewalls. By monitoring and documenting access and activity, you better enable your firm to catch security incidents quickly and prior to significant damage occurring.

In 2013, the U.S. Government via the White House issued an Executive Order: "Improving Critical Infrastructure Cybersecurity."[1] The order references the growing concern over cybersecurity and the potential impact of cyber-attacks on the country:

"The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

In other words, the government wants communication around cyber threats to increase, and the same sentiment with reference to public and private companies was echoed in the SEC's 2014 roundtable. To be best prepared, dialogue should be created between all sectors – public, private and government – in order to facilitate communication and sharing of threat factors and actionable instruction. The fact is that we cannot adequately prepare to combat security risks without proper information sharing. By creating a security framework, both public and private companies, including investment management firms, can set standards for better communication.

To start, firms should identify standards and best practices relative to cybersecurity. We'll cover many of these as you read on through this whitepaper. Once initial practices have been identified, firms should create a framework to elevate those practices and implement a thoughtful approach to security. Finally, identify gaps where solutions are needed within your firm's infrastructure and policies and implement as such to protect your firm from cybersecurity incidents.

A HACKER'S TOOLKIT: CYBER SECURITY THREATS TO FINANCIAL FIRMS

External cybersecurity attacks come in all shapes and sizes, and oftentimes we never fully understand the root cause or the intended outcome of the threats. As the industry continues to keep its finger on the pulse of cybersecurity and we communicate about attacks and vulnerabilities – new and old – we learn more about what a hacker is really after and, therefore, how best to protect that information.

What types of information are hackers after?

Hackers infiltrate corporate technology environments for a variety of reasons. In the retail arena (such as in the case of Target, TJX and other scandals in recent years) the perpetrator may be seeking customer data such as credit card information or social security numbers. In the investment industry, it is more likely that a hacker will attempt to steal information on a firm's intellectual property, such as business plans, trading programs, market forecasts and investment strategies.

How are they infiltrating networks?

Experienced hackers – or "hacktivists" – use a variety of methods to infiltrate networks and gain access to sensitive information. Including denial-of-service attacks, phishing, malware and software vulnerabilities. Let's dive into these hacker tools.

Distributed Denial-of-Service (DDoS) Attack

One of the most common strategies used by hackers is distributed denial-of-service. DDoS attacks are "efforts to temporarily of indefinitely interrupt or suspend services of a host connected to the Internet." Typical DDoS attacks may involve overloading communications through a network to slow down resources or forcing network reboots. In 2013, the Internet suffered its most severe DDoS attack, one dubbed the 'DDoS that almost broke the Internet."[2] Spamhaus, a non-profit, anti-spam organization was attacked via open DNS resolvers that were inundated with traffic (up to 300GB per second). Following the incident, Spamhaus released a statement urging businesses to shore up their networks:

"Preventing attacks like these depends on two key technical measures. First, all networks should ensure that they do not allow traffic to leave their network that has 'spoofed' (forged) sending addresses. Without the ability to spoof traffic there would be no reflection attacks possible. Secondly, open DNS resolvers should be locked down and secured. These attacks should be a call-to-action for the Internet community as a whole to address and fix those problems."

Phishing

The act of phishing refers to a hacker "psychologically" attacking a victim by tricking them into taking an action that results in the victim either providing personal information (such as password information), opening up an infected attachment or responding to spam. In traditional phishing, cyber criminals send out messages to millions of users trying to infect as many users as possible. Spear phishing however, is much more targeted. Attackers will do extensive research on all individuals' profiles and accounts, as well as anything that is posted on a public form or blog. They will then send a customized message meant to lure the desired target to take a specific action.

Malware & Ransomware

The term malware encompasses a number of security threats that could negatively affect a business's network, including viruses, worms, Trojan horses and spyware. While each of these has its own nuances, they are all deployed with the intent to damage systems and networks, oftentimes with very little noticeable interruption.

One example of a malicious ransomware trojan that first caught the attention of firms in September 2013 is Cryptolocker. Cryptolocker is a variant of ransomware that restricts access to infected computers by encrypting them and demanding that the victim pay the attackers a ransom in order to decrypt and recover their files. Some versions of Cryptolocker can encrypt local files as well as external hard drives, network file shares and even cloud storage services that allow local folders to sync with online storage.

Regular file and server backups become critical in cases such as this as infected computers need to be restored back to a point before the ransomware was installed in order to avoid paying the ransom. This highlights the importance of firm's taking a holistic view when creating security and data protection programs.

Software Vulnerabilities

Another vulnerability hackers love to exploit is out of date software. A perfect example: on April 8, 2014 Microsoft officially ended support of its outdated operating software, Windows XP. With the end-of-life date public, it is widely expected that hackers have been holding Windows XP-related malware just waiting for the day to come – and it has. That said, Microsoft did announce it will continue to provide updates to its antimalware signatures and engine for Windows XP users through July 14, 2015. However, the company cautioned that its research shows that the effectiveness of antimalware solutions on out-of-support operating systems is limited.

The Heartbleed Bug, which was made public in April 2014 but existed for up to two years prior, is another example of how technology weaknesses provide hackers opportunities. Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library that allows anyone on the Internet to read the memory of the systems protected by vulnerable versions of the OpenSSL software.

Mobile Devices

In today's smartphone-reliant world, hackers are shifting their focus and resources to mobile devices. With a user's life virtually captured within a single phone or tablet – everything from contacts and email to documents and passwords – hackers recognize the value of such devices. Some would argue mobile devices now hold as much as or more personal information than PCs or laptops, and most do not come standard with anti-virus or malware protection software.

In early 2014, Apple was forced to release a critical update to its new iOS7 operating system after a flaw was identified that could give an attacker with a privileged network position the ability to capture or modify data in sessions protected by SSL/TLS (a.k.a. public key encryption). Following that announcement, researchers at a cybersecurity firm (FireEye) published a proof of concept for a surveillance app that, if created and distributed by hackers, could capture every tap on an iPhone's screen. The information captured, including passwords and credit card numbers, would be accessible to the attacker. These are just two examples of the cybersecurity threats facing mobile devices. Users need to be aware that these threats exist and practice smart computing on all devices.

BEST PRACTICES: BUILDING A SECURE INVESTMENT FIRM

Hackers are always seeking new ways to gain access to protected systems and accomplish their goals. Anti-virus and anti-malware developers are likewise on the hunt for ways to protect these systems and data from new intrusion methods. To increase protection, hedge funds and investment firms should employ a Defense in Depth strategy. This includes maintaining up-to-date anti-virus and anti-malware software as well as network firewalls, deep inspection proxy and intrusion detection and prevention systems (IDS/IPS) to reduce the amount of traffic on the network.

It also means taking into account physical and virtual security elements. Following are items to consider from a physical security perspective:

- 24x7x365 manned lobby with visual verification of identity
- Two-phase authentication of visitors (card and biometric)
- Secured access doors and elevator banks
- Monitored security cameras
- Additional door, motion and camera sensors
- Visitor logs for cages
- Key-locked cages and cabinets

At the virtual level, monitoring becomes essential. Work closely with your IT department or cloud services provider to ensure they have comprehensive control and extensive visibility over your infrastructure at all times. You need to ensure it is highly secure and cannot be penetrated by external attackers or easily manipulated by internal threats.

In addition to these layers, investment firms should also employ the following policies and procedures to ensure their critical systems and data do not fall into the wrong hands.

Principle of Least Privilege

This involves restricting access to only those employees who need it. Keep access control lists on all applications and data and inbound/outbound Internet access to keep track of who can gain access to what. Also, log the use of audited one-time passwords and minimum-privilege shared accounts.

Secure User Authentication Protocols

Secure user authentication protocols should include:

- Assigning unique domain user IDs to each employee
- Implementing strong domain password policies
- Monitoring data security passwords and ensuring that they are kept in a secure location
- Limiting access to only active users and active user accounts

Access Control Policy

The first step you need to take is determining who at your firm needs access to what. The truth is not every employee should be able to access every file, server, etc. within a company. Firms should only authorize access to employees who need it. The less access employees have, the less damage can be done. After access is controlled, be sure to keep a log monitoring who has accessed what. Conduct a regular audit to determine what access levels are in place and what changes need to be made. When an employee leaves or changes roles, their access should be adjusted (or revoked) accordingly.

Acceptable Use Policy

What exactly is acceptable behavior for your employees as it relates to their technology usage? It's best to be specific within your Acceptable Use Policy regarding what activities and programs employees are or are not permitted to access. Some firms disallow access to social media sites, personal email and more while others are more open regarding access.

Firms can employ web filtering practices to block access to identified websites. Additionally, they can use third-party software to log activity around which employees are accessing what and what other actions they are taking (e.g. printing, copying, forwarding, etc.).

Incident Response Policy

Develop a plan that details how the firm will handle a security incident. The plan should outline:

- Who is in charge of managing a security incident,
- Required reporting and investigation procedures,
- Communications policies for contacting clients, other key stakeholders and regulatory bodies, and
- Post-incident remediation procedures.

We'll talk more about creating an incident response plan later in the report.

Visitor/Contractor Premise Access Policy

It is essential that firms keep track of all people who have visited the site through the use of physical security checkpoints and surveillance.

Mobile Device Policy

Develop guidelines for use of personal mobile devices in the workplace, and train staff on mobile device security. As part of your firm's personal communications policy, be sure to include language on what is considered acceptable behavior when it comes to using mobile devices (whether company-owned or as part of a BYOD practice). Questions to consider include:

- Is there a limit to data usage? Is texting allowed?
- What devices are supported? Are there restrictions what applications can be installed?
- What procedures are in place if an employee loses his or her device?
- Does the company have permission to remotely wipe the device of all content?

Make sure your employees understand exactly what the protocols are for using company or personal devices for work purposes.

FIVE HELPFUL SECURITY TIPS:

1. Patch applications such as Adobe PDF viewer, Adobe Flash Player, Microsoft Office and Java. Using the latest versions of these applications – and patching within two days – will help to prevent high-risk vulnerabilities. The same goes for your operating system.

2. Minimize the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.

3. Employ application white-listing to help prevent malicious software and other unapproved programs from running. Examples are Microsoft Software Restriction Policies or AppLocker.

4. Use a host-based intrusion detection/prevention system to identify anomalous behavior, such as process injection, keystroke logging, driver loading and call hooking.

5. Provide user education regarding Internet threats and spear phishing socially engineered emails. Avoid using weak passwords, password re-use, exposing email addresses, and use of unapproved USB devices.

A FEW MORE BEST PRACTICES

To round out best practices around managing and maintaining a secure hedge fund, we recommend the following to provide additional safeguards against cyber intrusions.

Perform a vulnerability assessment. It is essential that companies authenticate firewall configuration and anti-virus patching, network device security and evidence of criminal activity. You'll want to know where vulnerabilities exist before implementing additional security measures.

Engage real-time intrusion detection/mitigation solutions. Be sure to track and observe all network actions to be aware of breaches, attacks or the access of sensitive information.

Establish legal safeguards. Companies should ensure that they utilize confidentiality, non-disclosure, non-competition and non-solicitation arrangements to protect intellectual property.

Know who you're hiring. Employers should screen employees pre-hire and conduct trainings to make all employees aware of appropriate and inappropriate conduct, contractual arrangements and firm policies and procedures.

Monitor and log network activity. Restrict electronic transfers, enforce password protection, encrypt computer systems, and limit accessibility

CYBERSECURITY INCIDENT RESPONSE: WHAT NOW?

Even if you've been successful at implementing all of the security measures and protocols above, there is no guarantee your firm will avoid becoming the victim of a cyber-attack.

With the threat of security incidents at all all-time high, staying proactive is the best way to thwart potential damage. That means preparing how to respond to an incident when it does occur is also necessary. Here is a step-by-step guide to follow in the event your firm suffers from a security breach.

1. Establish an Incident Response Team.
Choose a select group of individuals to comprise your Incident Response Team (IRT). Assign each member a predefined role and set of responsibilities, which may in some cases, take precedence over normal duties. The IRT can be comprised of a variety of departments including Information Technology, Compliance and Human Resources.

2. Identify the type and extent of incident.
Before your IRT can alleviate any incidents, it must clearly assess the damage to determine the appropriate response. For example, if the incident is a computer virus that can be quickly and efficiently detected and removed (and no internal or external parties will be affected), the proper response may be to document the incident and keep it on file. This task could effectively be handled by the IT department.

If however, an incident occurs that affects multiple clients/investors/etc., the incident should be escalated to the IRT.

3. Escalate incidents as necessary.
Certain departments may be notified of select incidents, including the IT team and/or the client service team. These parties should use their discretion in escalating incidents to the IRT. Any event suspected as a result of sabotage or a targeted attack should be immediately escalated.

4. Notify affected parties and outside organizations.
One member of the IRT should be responsible for managing communication to affected parties. Depending on the severity of the incident, the IRT member will act as the liaison between the organization and law enforcement.

5. Gather evidence.
When appropriate and necessary, the IRT is responsible for identifying and gathering both physical and electronic evidence as part of the investigation.

6. Mitigate risk and exposure.
A technical member of the IRT should be responsible for monitoring the situation and ensuring any effects or damage created as a result of the incident are appropriately repaired and measures are taken to minimize future occurrences. The IRT will also need to define any necessary penalties as a result of the incident.

DON'T FORGET ABOUT MOBILE SECURITY

Earlier in this report, we touched on mobile device security and the inherent risks posed as a result of employees using their smartphones and tablets as much as if not more than traditional PCs and laptops. With trends such as bring your own device (BYOD) gaining traction across the enterprise, organizations fundamentally lose control over the hardware, how it is used and must ask the question how the company can be affected. Governing the fine line between personal and professional use on the same device can be challenging. But without clearly defined policies in place companies are making themselves vulnerable to a number of security risks.

For instance, 48% of respondents in an InformationWeek survey indicated that employees within their organizations had their mobile devices lost or stolen in the past year, with 12% of those cases requiring public disclosure, causing inevitable harm to the business. If proper security measures are not in place, the information contained on that device could become accessible to unauthorized parties and the company's reputation may suffer irreparable damage.

Additionally, there are many security risks involved in using one's personal device for business purposes that most users may not even be aware of. Many popular smartphone apps, such as public file transfer services, could allow sensitive information to be easily intercepted. Other common activities that could result in leakage of sensitive data include using personal devices to automatically forward work emails to public webmail services and using smartphones to create open Wi-Fi hotspots. Both of these practices make a company's data extremely vulnerable to hackers.

Mobile device management is a critical aspect of the BYOD policy. Be sure to directly state which rights the firm will retain with regard to provisioning mobile devices. Provisioning may include carrier activation, as well as installation of encryption technologies, various software tools, security certificates, anti-virus and more.

Other items to consider within this section are:

- Password and screensaver policies
- Blocking or removal of specific applications
- Encryption policies
- Process and timing of security scans
- Procedures for taking inventory of mobile device data and applications

CONCLUSION

The world of cybersecurity continues to change on a daily basis, and there's no telling where or when the next attack will strike. The best way to protect against an external attack or internal breach is to work with your internal security team or outsourced technology provider to structure and implement a sound security program to protect your firm's data and information as well as offer peace of mind to your investors. As a final takeaway, following are four tips to remember as you go down the path of shoring up operations and security practices:

1. Establish and implement an **Information Security Policy** that outlines the layers of security you will put in place from technology and authentication protocols to restricting access and password requirements;

2. Create an **Incident Response Plan** so you are fully prepared should a security breach or cyber-attack occur;

3. Train your employees on **Information Security Awareness** because a firm's security strategy will only work if employees are properly trained on it; and

4. **Conduct Due Diligence** on your service providers so they do not expose you to unexpected risks.

[1.] White House Executive Order -- Improving Critical Infrastructure Cybersecurity, February 2013

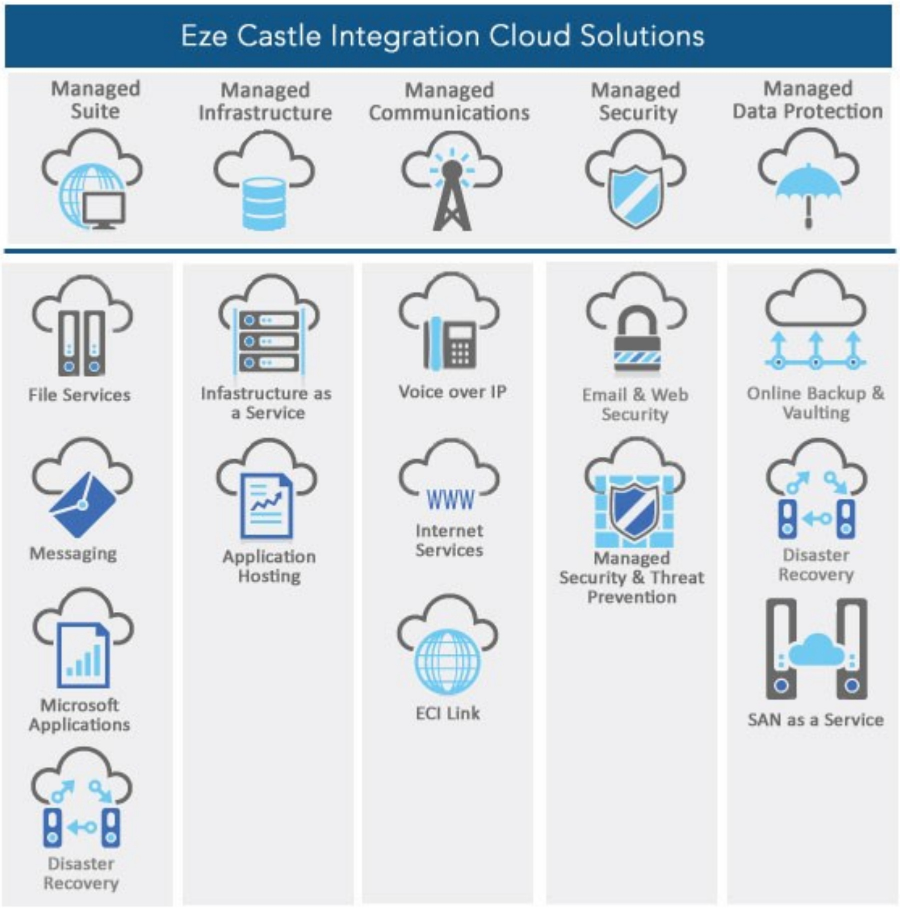
[2.] "Denial-of-Service Attack." Wikipedia: The Free Encyclopedia.

ABOUT EZE CASTLE INTEGRATION

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 650 alternative investment firms worldwide, including more than 100 firms with $1 billion or more in assets under management.

The company's products and services include Private Cloud Services, Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

To learn more about Eze Castle Integration, contact us at 800-752-1382 or visit www.eci.com.


Eze Castle Integration Cloud Solutions
Managed Suite
Managed Infrastructure
Managed Communications
Managed Security
Managed Data Protection
File Services
Messaging
Microsoft Applications
Disaster Recovery
Infastructure as a Service
Application Hosting
Voice over IP
WWW
Internet Services
ECI Link
Email & Web Security
Managed Security & Threat Prevention
Online Backup & Vaulting
Disaster Recovery
SAN as a Service