EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

Preventing Devastating Data Loss with the Evolve IP Prem Extend™ Suite of Disaster Recovery and Business Continuity Solutions

This white paper outlines the current cyber-threat landscape and explains how secure-cloud solutions like Evolve IP's Prem Extend Disaster Recovery Suite help companies rapidly respond and survive. The result is comprehensive protection of confidential data, prevention of business disruption, and a powerful defensive stance against cybercriminals and natural disasters, and infrastructure failure.

Overview

Companies face unending stress from a constantly evolving marketplace. Now, they are also facing an insidious foe: Ransomware – computer malware that makes the victim's data inaccessible until a high ransom is paid. Sophisticated criminals encrypt the victim's files and demand a payment to decrypt them. The payoff for hackers can be huge. The Federal Bureau of Investigation estimated that in just six months, the extortionists behind the 2014 CryptoLocker strain of ransomware swindled $27 million from people whose data they took hostage.[1]

This dastardly digital deed is not new. As far back as 1989, the AIDS Trojan virus infected 20,000 diskettes disseminated to attendees of the World Health Organization's international AIDS conference. In 2006, the Archiveus Trojan encrypted everything in the "My Documents" directory on a system and required users to make purchases from specific websites to obtain the password to decrypt the files. Since then, this corporate crime has grown increasingly more sophisticated (more strains, more potency) with the potential to inflict ever-greater harm – a 25% growth in ransomware "families" is expected this year.[2]

The most critical element of a disaster recovery plan is the recovery time objective, or RTO. In essence, no matter what the cause of an outage, the critical question is how long will your company or facility be down?

"Ransomware is capable of crippling organizations that face it, and the cybercriminals spearheading these attacks are creatively changing on a continuous basis to keep enterprises guessing," says Raimund Genes, chief technology officer at Trend Micro.[1]

"While it is unfortunate for us, cyber criminals are resilient and flexible when it comes to altering an attack method each time we find a patch or solution," added Ed Cabrera, chief cybersecurity officer at Trend Micro. "This creates massive problems for enterprises and individuals alike because the threats change as often as solutions are provided."[1]

Indeed, the threat is serious and far-reaching. Ransomware attacks quadrupled in 2016 – between 2 million and 3 million attacks took place, extorting $1 billion in payments.[1]

"Ransomware presents an easier and safer way for hackers to cash out," says Experian's 4th annual Data Breach Industry Forecast." Given the potential disruption to a company, many organizations will opt to simply pay the ransom. This has unintended consequences of funding more research and development by attackers who will in turn develop more sophisticated and targeted attacks."

In addition, one survey ranked the negative effects of ransomware attacks on businesses saying that more than two-thirds (78%) of stakeholders are significantly impacted.[3] According to a 2017 SMB Insights survey, 60% of U.S. businesses with between one and 499 employees shut down 6 months after suffering a data breach. [3]

IMPACT OF CYBER ATTACKS ON SMALL AND MID-SIZED BUSINESSES

• Number of Businesses with 1 - 499 Employees	**7.8 Million**
• Victims of a cybersecurity breach	**16%**
• Close their doors within 6 months of the data breach	**60%**
• Estimated Number of Closings	**749k**

But Wait, There's More …

While ransomware is one of the most highly publicized and damaging threats to a company's IT infrastructure, there are many more menacing types of potentials for disaster. Physical disasters churned up by Mother Nature, for example, have wreaked havoc in recent years. In fact, research by the University of Texas shows that only 6% of companies that suffer a catastrophic data loss survive, 43% never re-open, and more than half close within two years.

For example, Hurricane Sandy in 2012 which downed 74% of small businesses in New York City, New Jersey, and Connecticut. Apria Health Care – a national provider of oxygen tanks and other medical supplies and services to homes of elderly, incapacitated, and convalescing patients – was squarely in Sandy's destructive path but continued "business as usual" by leveraging disaster recovery services from Evolve IP to receive calls and ensure critical supplies would reach customers.

"Evolve IP protects a business from much more than just the impact of severe weather in one area of the country which, in our case, affects each branch a few times per year, usually for a few hours at a time," explained Jeannine Delivron, Apria's New York Area operations manager. "More significant is the fact that the Evolve IP system provides total emergency capabilities when we have to close down completely and re-route calls – a situation that happens two or three times each winter for branches in the Northeast and that could be devastating to our patients if we were not prepared. Instead, we completely avoid a disaster."

In addition to natural phenomenon, companies must prepare for all forms of disaster. Here are some of the most common that are often overlooked:

1. **Hardware/Connectivity Failure** – While most modern technology is fairly robust, no company is immune to hard disk or Internet connection failures. While it can be costly to eliminate any single point of failure in the IT infrastructure, having a disaster recovery plan that does this is the only way to ensure that a hardware failure doesn't interrupt service or cause data loss.
2. **Human Error** – Human beings aren't perfect. While common, human mistakes can often be the hardest to prevent and correct. It's important to ensure systems are backed up incrementally so staff can easily restore files to an error-free state. Redundant firewalls and anti-virus and anti-spyware software can also ensure that security breaches are protected if an employee accidentally leaves a port open, for example. Continuous staff training is vitally important.
3. **Non-Ransomware Cyber Attacks** – Experian predicted that healthcare organizations will be the most targeted sector for cyberattacks in 2017, "with new sophisticated attacks emerging." While ransomware is still the most ominous form, cyberattacks come in hundreds of different disguises and, as such, are very difficult for organizations to prevent. Also, as more institutions deploy new mobile applications, they may introduce new vulnerabilities.

"The most important steps in protecting your company's and your customers' data from the growing threat of malicious cyber attacks are ensuring that you have a robust back-up and recovery process, and that your security software is up-to-date and able to detect the most recent ransomware variants," said Rob Kraus, director of research for Solutionary's Security Engineering Research Team. "As the threat continues to grow, it will be crucial for organizations to have defined incident-response procedures and proper detective and preventive controls in place to reduce negative impact."[5]

Back-Up Is Not Enough

While companies typically invest in a wide range of disaster recovery-inspired back-ups, redundancies, and other failover mechanisms … it's usually not enough. In reality, only a tiny fraction of companies can afford to maintain a fully mirrored system running in a remote location, receiving a real-time stream of data, ready to pick up where another leaves off in a few milliseconds. Of course, there are many ways to recover systems that are less expensive than a complete live duplicate, and each organization decides what level of recovery it needs – striking a balance of cost vs. risk. However, modern cloud-based networks with redundancy and failovers for both data and voice like Evolve IP's offer a cost-efficient alternative that gives businesses the best of both worlds: low cost and world-class security, availability, and performance.

To guard against ransomware attacks and ensure business continuity, organizations must employ various safeguards that protect the integrity of their network, systems,
and data:

1. **Protect endpoints –** Use endpoint protection with advanced features. In many cases, a protective system is installed with only default features enabled. By implementing advanced features, more malware can be detected and blocked.
2. **Employ antispam –** Most ransomware attacks start with a phishing email that contains a link or a certain type of attachment. For phishing campaigns that pack ransomware in an uncommon file format, it is easy to set up a spam rule to block these attachments.
3. **Block unwanted or unneeded programs and traffic –** Block the application and its traffic on the network. Doing this can stop the ransomware from getting its public RSA key from the control server, thereby blocking the encryption process.
4. **Leverage a virtual infrastructure –** This provides backups for critical systems by making them "air gapped" from the rest of the production network. It also ensures that backup systems, storage, and tapes are in a location that is not accessible by production networks.
5. **Perform ongoing user-awareness education –** Since most ransomware attacks begin with phishing emails, user awareness is critically important. Statistics show that for every ten emails sent by attackers, at least one will be successful. Employees must not open emails or attachments from unverified or unknown senders.
6. **Ensure Rapid Recoverability –** The most critical element of a disaster recovery plan is the recovery time objective, or RTO. In essence, no matter what the cause of an outage, the critical question is how long will your company or facility be down? If you get attacked have a server failure, is data recoverable and can backup servers be immediately accessed? Guaranteed recoverability of critical systems is essential to ensuring that the business and the customers experience minimal disruption or discomfort.

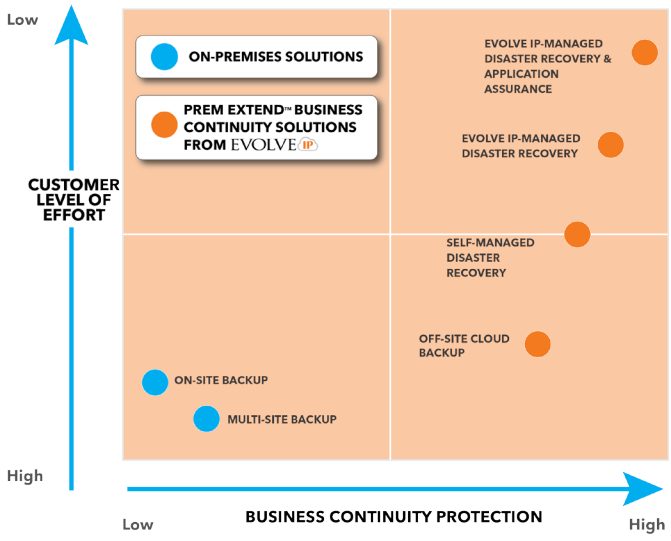
Rapid Recovery Case Study: Managed Recovery in the Cloud

To illustrate how the cloud can help mitigate ransomware attacks, consider a recent example in which an Evolve IP customer was hit by the CryptoLocker virus. The virus, which successfully encrypted many of the company's production files, proliferated when an employee inadvertently clicked on an infected email, allowing the virus to fly through the company's systems.

As soon as the company realized it had been attacked, it alerted Evolve IP's managed DRaaS (disaster-recovery-as-a-service) response team. This alert initiated an immediate analysis of the back-up file library to identify the recovery point closest to the point of impact (the time when the files were encrypted by the attacker). Within just 80 minutes, Evolve IP's managed services engineers pinpointed the first sign of data corruption and began to return the full customer environment to its original status using uninfected backups. This included 33 virtual servers and 10 TB of data. Evolve IP restored all of the servers from the geographically redundant cloud backups. This process involved powering down the infected servers and powering-up the new environment, including testing to ensure complete application functionality and data access.

The reason for this "rapid recovery" success was Evolve IP's great technical preparation, including having an experienced response team at the ready. As part of the managed DRaaS solution, Evolve IP captures data snapshots around the clock on a rolling 15-minute schedule to create a library of 96 backups every 24 hours from which customers' systems can be recovered. Further, an independent supplemental data backup procedure – using a different backup methodology – backs up the customers' environments each night. Thanks to Evolve IP's managed DRaaS solution, the customer did not lose any data and maintained full business continuity.

Evolve IP Prem Extend™ Suite of Disaster Recovery and Business Continuity Solutions



Recovery and Production: Better in the Cloud

Evolve IP delivers secure, audited and PCI compliant cloud-infrastructure to protect healthcare companies from any threat. By moving enterprise applications and infrastructure to Evolve IP's world-class cloud, companies can ensure that their applications are available from any location, regardless of what is happening at their office. In contrast to the traditional on-premise, do-it-yourself model in which an organization must continually re-invest in its own systems, data centers, and infrastructure, Evolve IP provides software, hardware, and architecture to guarantee business continuity and survivability against breaches.

The cloud is superior to the traditional on-premise model for these reasons:

- **Environmental Protection –** If a company's on-site data center loses power or employees cannot access the physical building for any reason, the business may stop or significantly slow down. Applications that are run in the cloud – and properly backed-up in various locations – enable an "always-on" environment.
- **Network Protection –** If power is out, the network is usually out, but networks can still be down when power is restored. Aging infrastructure or poorly constructed network hubs can wreak havoc on networks, and consequently, customer service levels. In contrast, well-architected networks in the cloud provide a variety of pathways to access network data and applications.
- **Business Applications and Data Protection –** All enterprise business systems should adhere to guidelines for Recovery Time Objective (the maximum duration of time allowable for complete system restoration), Recovery Point Objective (the maximum allowable time period from the disaster to the last backup), and Network Uptime Objective (the percentage of time a system should be available or "up"). Cloud technology that houses all systems off-site ensures that an enterprise stays within these guidelines.

You're Only as Strong as Your Weakest Link

The age-old saying is as true today as ever. No business is immune to IT disasters but there are many ways to safeguard against them and strategies to enable a fast and full recovery. The first step is to evaluate your current disaster recovery plan to ensure production servers are located in a top-tier data center with no single point of failure on the power and network connections. Disaster recovery backup servers should be at another datacenter – geographically diverse from your production servers – in case of a severe natural disaster. Follow this link to see Evolve IP's sample disaster recovery plan document.

For more information on Evolve IP's proven, cost-effective, and reliable suite of products that meet a variety of recovery time and point objectives, visit http://www.evolveip.net/draas-suite.

Sources

1. FierceHealthcare.com, "Cybersecurity: What 2016 Taught the Healthcare Industry," 2016. For more: http://www.fiercehealthcarecom/it/feature-cybersecurity-what-2016-teaching-industry

2. CSO Online, "The History of Ransomware," 2016. For more: http://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html

3. "Understanding the Depth of the Global Ransomware Problem," Osterman Research, 2016. For more: www.ostermanresearch.com.

4. Philadelphia Business Journal, "Survey: Cloud Computing has business owners attention while cybersecurity concers tick lower," by David Arnott, April 4, 2017. For more: http://www.bizjournals.com/philadelphia/news/news-wire/2017/04/03/survey-cloud-computing-has-business-owners.html

5. Becker's Hospital Review, "Hospitals Are Hit with 88% of All Ransomware Attacks," 2016. For more: http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html

About Evolve IP

Evolve IP is The Cloud Strategy Company™. Designed from the beginning to provide organizations with the ability to deploy both cloud computing and cloud communications onto a single platform, today, nearly 200,000 users rely on Evolve IP for services like disaster recovery, contact centers, unified communications, virtual desktop services, IaaS and more. With deployments across the globe, Evolve IP provides cloud services in virtually every industry with specializations in the healthcare, finance, veterinary, retail, legal, and insurance verticals.