Recovering IT and the business from extreme destructive incidents
Recovering IT and the business from extreme destructive incidents
Cyber attacks have evolved beyond limited-impact nuisances into sophisticated, targeted attacks backed by well-funded, so-called state-sponsored terrorism or industrial espionage groups – with devastating effects. These threats and attacks – and their destructive capabilities – are further evolving, causing enterprises and governmental organizations to grind to a halt and forcing most observant IT units to develop ways to mitigate these new risks. Major incidents have been reported at hospitals, universities, manufacturers, pharmaceuticals and government agencies in Britain, China, Russia, Germany, Spain and other countries.

Organizations are continuing to put measures in place to harden their networks, protect their perimeters and implement tools that alert their operations teams to nefarious or abnormal activity. While these measures are important and protect organizations against a large number of attacks, they always remain susceptible to a single vulnerability and increasingly lag behind the evolution of threats. Organizations need to prevent attacks and also prepare for recovery from successful attacks.

This article will walk through additional steps that an enterprise should consider taking to help focus on protecting its IT infrastructure. It will provide an infrastructure approach designed to defend against extreme destructive incidents, with a framework that integrates business continuity, disaster recovery and crisis management. The framework also helps in addressing the people, processes and technology needed to respond and recover once existing preventative networks, systems or infrastructure have been breached.
What is the issue?

Organizations have realized that they are not prepared to withstand advanced and evolving threat attack vectors. Developing a resilient solution that complements the organization’s security prevention, detection, and traditional business continuity and disaster recovery efforts is now paramount. We continue to see different and changing extreme destructive incidents that impact the enterprise’s ability to conduct business. These extreme destructive incidents can include:

- Ransomware (data is encrypted – victims are ordered to pay ransom)
- Wiper ransomware (ransomware masquerading as safe is sent to wipe data out)
- Data manipulation (business discovers changes in data values)
- Cyber-physical attack (infrastructure is physically destroyed)
Enterprise IT infrastructures are gradually growing in size, and their interdependencies are becoming more complex because of emerging technologies such as the cloud, Internet of Things (IoT), mobile devices, collaboration platforms and social platforms in this digital transformation era. While these technologies provide opportunities for enhanced productivity, improved decision-making and data-supported insights, they also broaden the scope of potential security vulnerabilities.

Modern-day cyber threats and attacks are not limited to viruses or malware that is injected into enterprises to infect user data. Today, we are witnessing sophisticated, ever-evolving attacks by cyber criminals and state actors seeking to distract enterprises and manipulate, destroy, wipe and lock access to their most important data. We call such successful attacks “extreme destructive incidents.”

While advanced security suites such as enterprise edge protection, threat intelligence and advanced endpoint protection may help prevent some of these attacks, it is impossible to address each and every new, evolving threat that appears on the cyber-attack landscape. Organizations lack solutions to either prevent these attacks or recover from attacks. Also, many enterprises do not have the resources, experience and investment capital needed to combat modern cybercrime.

How does this impact you?

Although they were equipped with state-of-the-art cyber protection technologies supported by skilled resources and defined processes, several prominent organizations have found themselves in severe data-loss situations after attacks in recent years. Recovery has been slow. In multiple instances, these attacks had self-propagated with enterprise-wide impact, incapacitating not just production environments but also disaster recovery environments within minutes. Extreme destructive incident situations leave organizations paralyzed and unable to access information systems to conduct business. As enterprises increasingly depend on data for day-to-day activities and insights, being prepared for these incidents is paramount.

When it comes to business disruptions or outages of any sort, every minute of downtime impacts businesses exponentially. For example, a ransomware incident’s harm goes beyond data losses for an enterprise and its customers. It forces the company to spend more time (weeks and months, not days) and resources to recover because traditional business continuity, disaster recovery and crisis management programs are not ready or structured to respond to these attacks.

---

What's the fix?

While most organizations are heavily investing in cybersecurity suites and applications, it is also extremely important to explore and invest in a framework that addresses the people, processes and technology as the safety net and last line of defense in the event of the worst-case scenario. In concert with prevention and detection, this framework would support an enterprise’s response and recovery of data, applications and, ultimately, business from an infrastructure perspective.

The framework would address recovery from extreme destructive incident situations such as ransomware attacks, data theft and hostage, data wiping, infrastructure destruction and long-term data manipulation. Its associated approaches would be used only when all other means of recovery (e.g., data backups, regeneration and disaster recovery) have been rendered incapable or are unusable. This could happen either because the other recovery methods were infected or because it would take too long after the time of infection to activate the approach.

The framework would address the technology aspects with data protection measures that involve keeping secure, “point-in-time” copies of vital enterprise data in a “vaulted” environment, which is typically isolated from the main production network through an “air gap.” Periodically, restricted connections are made between the vault and the production environment to make such point-in-time copies. In the event of a recovery, these approaches only allow access to protected data through a physical presence in the vault, thus effectively protecting the vault from malicious code that spreads through the network. Several organizations have started embracing such approaches by keeping secure, point-in-time copies of their critical enterprise data. If these enterprises need to recover from recent, planned attacks and malicious code injections, they will be able to go “back in time,” in a sense, with access to uncorrupted files from up to two years ago.

In combination with the vault and the air gap, the framework would address the people and processes with a new, resilient governance structure, incident response and recovery procedures through the development of “operational runbooks.” Implementing an approach is the first step; sustaining it, adapting it to the changing threat landscape, and exercising and testing the recovery processes ahead of an incident are the necessary next steps. The operational runbooks prepare the organization for a vastly different recovery operation under these extreme destructive incident situations.
We have witnessed more and more enterprises being attacked by cyber threats. For an organization, it is now evident that the question is not if a threat will emerge, but when it will emerge. Recent years have seen a dramatic uptick in business data destruction, manipulation, access lock variants and wiper malware masquerading as ransomware, and the age of self-modifying, self-propagating ransomware is upon us. If you think your enterprise is immune, just look in the news to find examples of organizations that were impacted by these very real threats. This is clearly the race you don’t want to lose.

Investing in solutions and a framework that provides organizations a way to recover from extreme destructive incident situations when preventive measures fail is critical, and it is a logical step to take to mitigate risk to your business data and applications. Given today’s ever-evolving cyber-threat landscape, this approach will play a significant role in helping enterprises recover from a severe extreme destructive incident.
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2020 EYGM Limited. All Rights Reserved.
This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.