

Counter Attack: Cyber Attack



Prayers can do miracles but when it comes to cyber security having the right strategy can save the business. In last few years cyberattacks have increased multi-folds and these attacks are no more limited to big corporations or government organizations but cybercriminals have started attacking smaller business like retailers, hospitality business owners, healthcare providers and even educational institutes.

Small and medium business have no greater advantage of being safe from cyber threat. Both, small and medium businesses (SMBs) and large corporations are equally prone to cyber threat according to various studies. The issue of cyber threats and security breaches are often not taken seriously by SMBs and they have to discover it the hard way after the business gets hit by an unexpected malware attack that damages critical data for the company.

The mindset of small and medium businesses that hacker will be least interested to attack them is a myth. Hackers are aware that SMBs' lack resources, knowledge and skill to protect themselves from cyberattack hence it makes them more vulnerable. If we look at cyber-attack trends, it is clear that hackers have an affinity to small and medium business and as per the 2017 Cost of Data Breach Study: Global Overview, it has been discovered that 1 in every 4 SMBs face the threat of a cyber-attack for unknown reasons.

According to the Ponemon Institute, the average price for small businesses to clean up after their businesses have been hacked stands at **\$690,000**; and, for middle market companies, it's over **\$1 million**.

The research by Ponemon Institute *2016 State of Cybersecurity in Small and Medium-Sized Business*, finds out that **only 14% of businesses** covered in this research has shown ability to mitigate cyber threat as highly effective. It was also found that due to high adoption of cloud services and use of mobile devices have made these businesses more vulnerable to cyber security risk which will further put pressure on the resources.

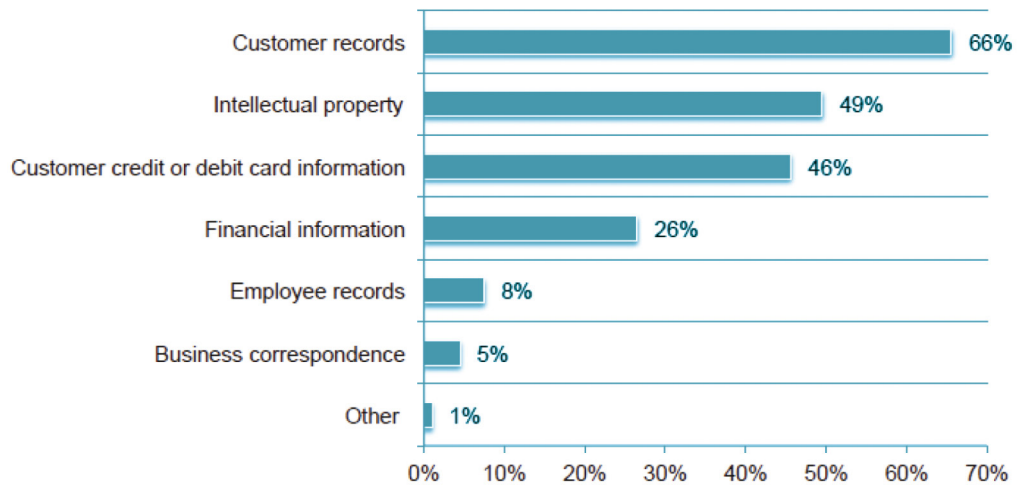
Motivation level for a hacker to attack varies from business to business. For instance, retailers are mostly attacked to get hold of personal and financial information of the customer and many small businesses are prone to attack to get access to their clients which might include details of large businesses. Moreover, there has been a rise in malware and ransomware forcing businesses to pay to get their data back. There has been instances where hackers have committed crimes related to filing of fraud tax refunds or health insurance

Over **75%** of the healthcare industry has been infected with malware over the last year

Healthcare industry is frequently targeted with 164 threats detected per **1,000** host devices

96% of all ransomware targeted medical treatment centers

What types of information are you most concerned about protecting from cyber attackers?



Source Ponemon Institute

One of the study has come up with the staggering figure that on an average there is one attack per 39 seconds. According to Pew Research, a majority of Americans (64%) have personally experienced a major data breach.

There is no industry vertical which is not vulnerable and as per the survey 75% of healthcare industry that includes medical treatment facilities, healthcare manufacturing and health insurance companies has been hit by malware. As per HIPAA

Journal, the year 2015 was a record setting year for healthcare industry data breach as the number records which were compromised in 2015 was much more than compared to last 6 years combined together. The year 2016 witnessed another high in healthcare data breaches than any other year and it seems that in year 2017 record would be sky high.

It has been observed by Core Technology that most of the SMBs targeted by hackers are ill-equipped to handle a security breach. The targeted enterprises failed to have appropriate defensive measures against a cyber-attack, even though the idea for a detection system was suggested at the conceptualization stage while laying the foundation of IT infrastructure. It is hard for SMBs to justify an expensive defense system early at the start of their business but hackers target an organization when the firewalls are weak or completely down, usually at the beginning of an enterprise, and hence timing is very important for proper security.

Healthcare manufacturing nearly reaches a **90%** malware infection rate

Healthcare has the **5th** highest count of ransomware among all industries

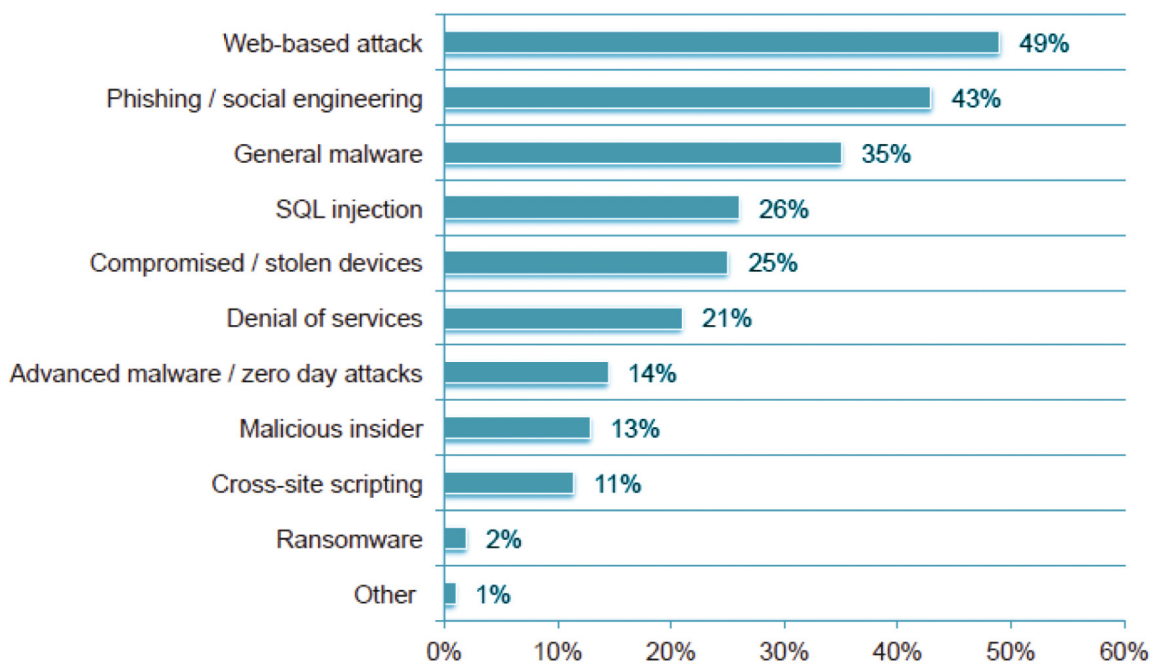
Over **50%** of the healthcare industry has a network security score of a C or lower

According to the research by IBM, it was found that the global average cost per record for a data breach is \$141 and the total cost of a data breach was \$3.62 million in 2017 in the US alone. On the positive side, this figure is 10% less than the previous year but the average size of a data breach increased by 1.8% this year, i.e. an increase of 24,089 accounts of cyber-attacks.

While selecting an IT services provider businesses look at the security management at vendor level and completely ignore IT security infrastructure and resources required within the company premises. There is a certain set of work which is required to be carried out at the end user level or client side for security management and maintenance.

Most of the smaller businesses are prone to web-based and phishing attacks. There have been scenarios where a data breach has taken place because of the negligence of the employee or other person working with the business. It has also been found that many businesses failed to identify the root cause of the attack. One of reason of easy vulnerability is that there is no function within the business to determine security priorities.

What types of attacks did your business experience



Source Ponemon Institute

Businesses must understand that the probability of threat is higher at the initial stages and the cost to recover from such attacks is significantly huge which may stall the progress of a new born business. Along with this, they must also learn about the factors that play a vital role to reduce or increase the impact and cost of data breaches.

Factors responsible for threat detection:

Visibility: Having a comprehensive visibility in a network, its activities and traffic flow helps to identify any malicious activity within a system. Detection of such grey areas and patching it with the right measure, in time, will prevent the possibility of larger security threat in future for an organization.

Monitoring: Today, it is a basic requirement for every major network to comply with the framework of PCI DSS, HIPAA, etc. to regularly monitor the incoming and outgoing traffic on critical devices. This is a measure to actively spot any suspicious changes in the nature of the traffic flow and thereby bring timely attention to malicious activities.

Compliance: Setting security measures as per the guidelines of the federal government can be another factor to ensure the safety of a company. This, in turn, helps to streamline the process and track all the changes that an enterprise experiences with changing time allowing ample opportunities to implement the necessary modification into an ecosystem for better security.

Tracking Trends: Looking out in the market for new methods of threat detection and countermeasures always help to achieve a good measure of security for SMBs. Decision making becomes easier and timely execution for threats becomes possible with current market trends.

For startups and SMBs, it is highly critical to save capital and therefore to deploy a world-class security system will shunt their growth. However, taking into account the above factors and building a security system with a sensible, cost-effective approach is enough to countermand threats in the beginning. CoreIT lists below a few tips that can save money as well as help SMBs to increase their response to threat detection and possible breaches:

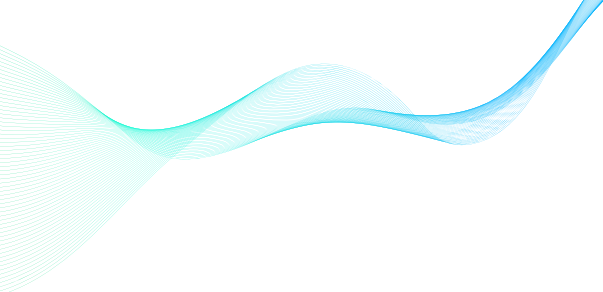
Skilled Personnel: Having skilled professionals that can make a sound decision and execute timely actions in event of a threat (or in advance) can save an enterprise from a lot of expenses that may occur after a breach.

Retainers: Setting up retainers by an experienced team of experts for an incident response can quickly identify and contain an attack. This is an important part of a detection plan that can help to avoid costly delays and must not be overlooked.

Response speed: Containment of a breach depends, for a significant part, on the time taken to identify the incident and the speed of response to implement a countermeasure. Logs and Error Report: Recording the incident, activities during the breach, errors generated, etc. can help to identify causes of the attack and save data from further threats.

Mitigation of attack: Resetting passwords, services, shutdown access to critical data, planning, etc. can prevent the access of attacker from seeping into the system further.

Internal Communication Plan: Communicating the incident internally in the most discreet manner till the system resumes can help to control panic. Also coordinating work with security protocols during a breach can help to maintain decorum and also speed up the recovery process.



Core Technology research has found that the top cost-reducing factor for a startup for threat detection, prevention, and security deployment is an internal or outsourced incident response team trained to contain cyber threats and data breach incidents. Data breaches are different for different industries and regions. In this scenario it is not possible to have a one-size-fits-all security solution. The requirement for each business varies depending on the regulatory compliance, internal IT infrastructure, linkage of IT strategy to business strategy and many more

Having a trained response team helps to monitor and accelerate the time frame in which security can help to contain a possible threat within reasonable cost. Keeping in mind the cost factor for most SMBs, Core Technology has come up with a comprehensive customizable information security plan with trained teams.

To enable a quick response, Core Technology focuses on laying out a ground plan that connects various parts of a complex ecosystem and estimates the threat possibilities with past data and anticipated threat analysis. Since the deployment of a security measure is tedious, we enable technical support right from the inception of a security plan so that we are in touch with the business processes that require maximum attention.

For all your queries about data breach, security protocols, compliance issues, etc. reach out to us today to have a look at the latest security measures for SMBs.



 1.212.271.8732
 info@coreitx.com
 www.coreitx.com

