Cybersecurity: What is Your Organization's Plan and Strategy?

61%

say their business was a victim of a cyber attack *(up from 55%)**

54%

say a negligent employee or contractor was the root cause of their data breaches *(up from 48%)**

33%

say an external hacker was responsible for their data breaches (*up from 27%*)*

32%

don't know the root cause of their data breaches (*same as the previous year*)*

*Ponemon Institute. "2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB).

In today's interconnected, always-on business environment, security and data protection are top of mind for all organizations. The growing culture of BYOD in the modern office touches business networks 24x7, expanding security vulnerabilities, opening new paths for data breaches.

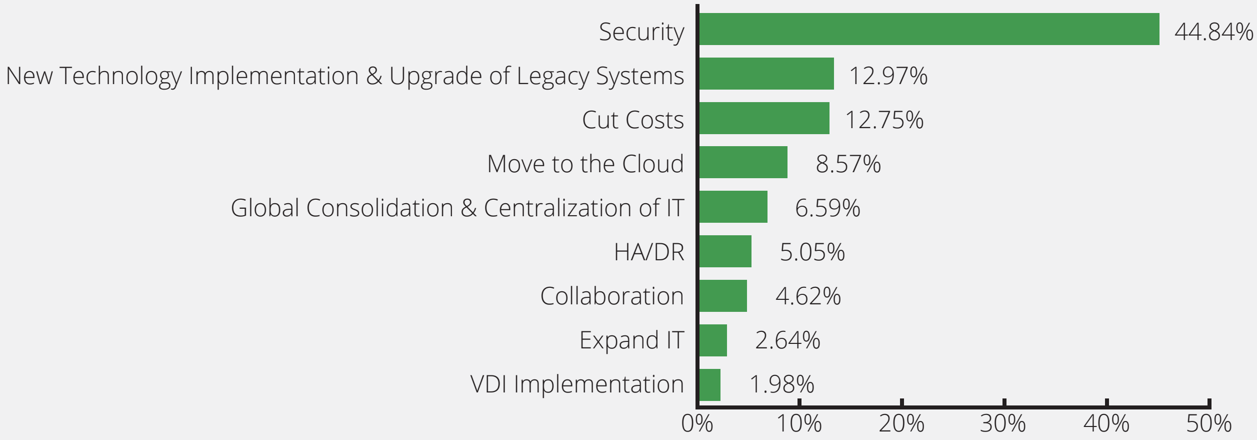
Advances in technology have transformed the corporate IT landscape. In the past, corporate computing was centralized, with data stored in-house behind a clear and defensible network perimeter. Today, IT teams are challenged with the complexity of cloud computing, management of mobile devices, evolving BYOD policies, remote workers, social media, and web services.

With digital transformation, the network perimeter has disappeared, and the attack landscape has expanded far beyond the office walls.

As data fuels the digital economy, the always-on, always connected user access opens security gaps. Security threats can be internal or external and the result can be disastrous. The tools and techniques for attack are sophisticated and there is a worldwide network of highly-evolved cybercriminals, who daily attempt to breach corporate networks with new methods of attack.

The threats to organizations are a real and present danger—51% of organizations surveyed have some or all of their infrastructure in the cloud and 64% have deployed virtualized desktop infrastructure to reduce their TCO (Total-Cost-of-Ownership). Email and web browsing have become the attack vectors of highest concern for their IT teams (ResearchCorp). As a result of the pervasive security threat landscape, 44.8% of organizations surveyed across the US view security to be their #1 priority—placing this ahead of other business-critical initiatives, such as new technology implementation, legacy system upgrade, cost reduction, and High-Availability/Disaster Recovery (Source: ResearchCorp 2017 U.S. IT Services Report).

IT Priorities



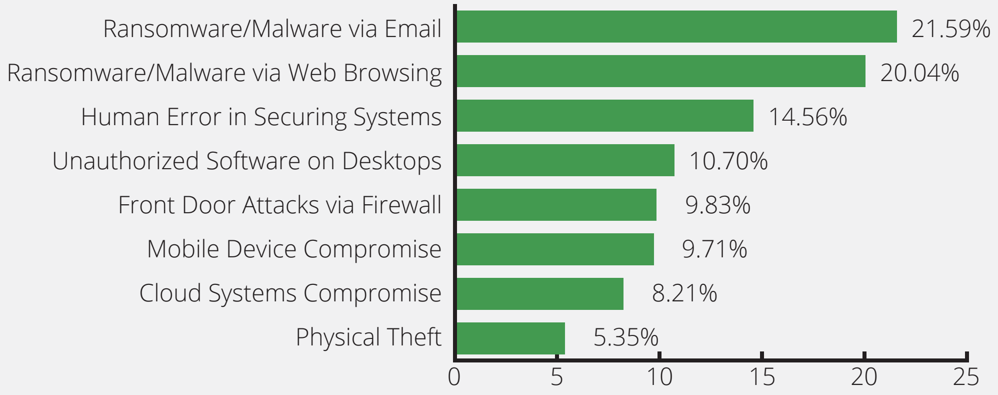
Sources: ResearchCorp

What threats are organizations most concerned about?

Data Breaches

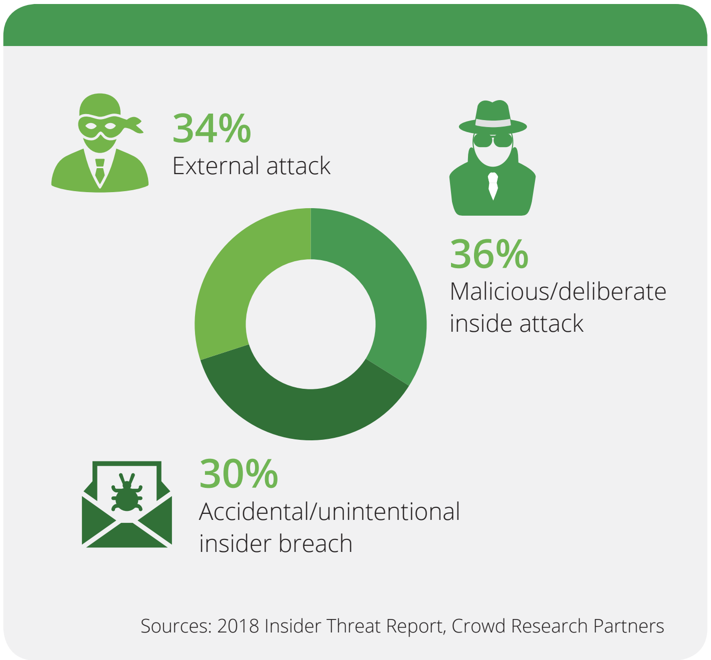
Cybercriminals troll the Internet 24x7x365 in search of organizational vulnerabilities that will allow them to breach your network and steal your valuable, sensitive, corporate data. According to the latest Insider Threat Report, 66% of intrusions are the result of insider behaviors. Cybercriminals prey on users and use this strategy as an easy way to gain access to the network. A comprehensive security strategy must account for: human error behavior and policies, systems and software maintenance, and update practices. Establishing a plan that accounts for these areas can substantially reduce the threat of a data breach and immediately reduce pathways for network intrusion and data loss. With security policies and procedures in place, ongoing review, update, and monitoring is an absolute requirement.

Attack Vectors of Concern



Sources: ResearchCorp

Human Error



Sources: 2018 Insider Threat Report, Crowd Research Partners

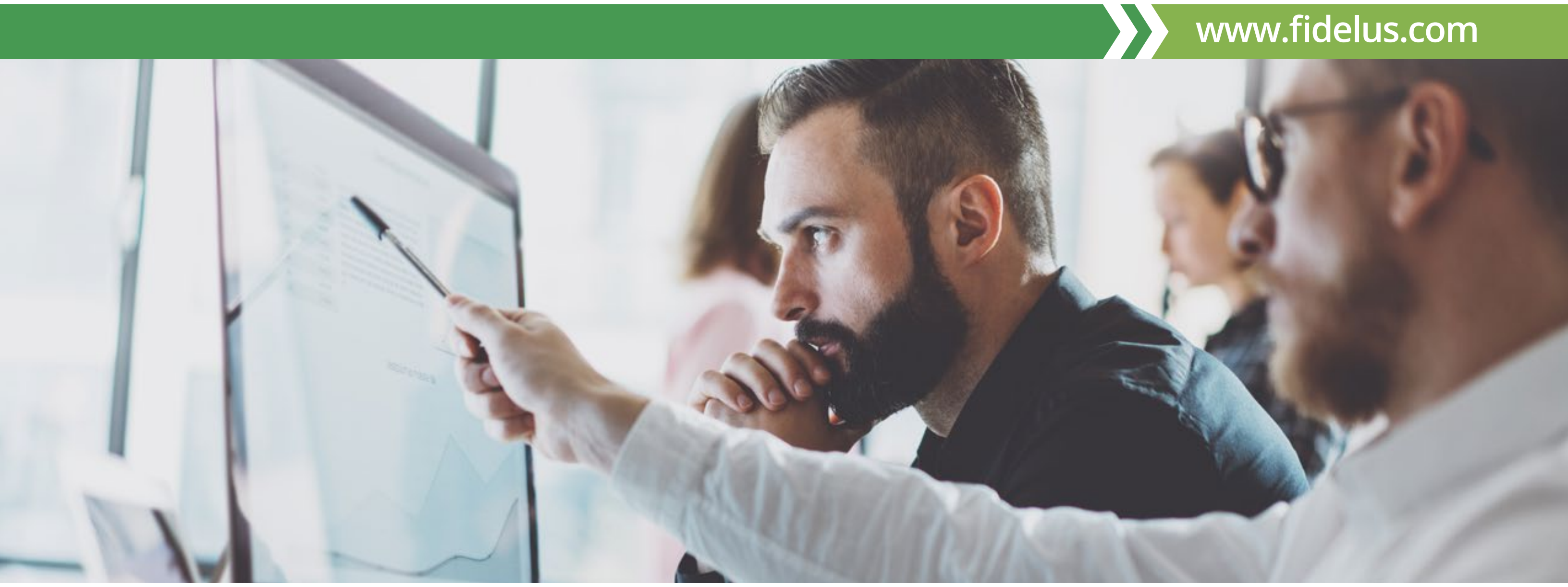
Unintentional human error accounts for 51% of all data breaches (2018 CRP Insider Threat Report). The easiest pathway into a network is through the laid-back handling of login and access credentials. Users must be trained to understand that their passwords should not be posted in an unprotected location or shared with others. In addition to not properly safeguarding information, weak and common passwords, regularly used across both professional and personal accounts, present a super highway for cybercriminals to breach corporate networks. Best practices regarding password privacy, strength, uniqueness, and an enforced change schedule can help remediate this attack vector. In addition, assuring databases and web servers are protected on premise, or in secure facilities off premise, will strengthen organizational security.

Employees should also be taught that both email and social media sites can contain malware. Clicking on links from any unknown source can infect an employee's computer, tablet, or mobile phone, and can open a path into the corporate network.

Unauthorized software on corporate computers is another area of network intrusion opportunity for cybercriminals. All too often, employees install non-standard applications onto their network connected devices. These applications can contain malware and open the organization's network to intruders. Best practices are to maintain an approved list of applications that employees can use on their devices and, as necessary, perform installation to assure integrity of the source download or sign-up.

The Disgruntled

Network intrusions and data theft from 3rd parties can occur directly or due to employee carelessness or ignorance of good security practices. Similarly, current employees who are unhappy or former employees who left under less than ideal circumstances, can also be a threat to an organization's security and currently account for 47% of network intrusions and data theft (2018 CRP Insider Threat Report). The result of an intrusion, especially when a formerly trusted person chooses to actively hurt the organization, can be disastrous. The optimal approach to maintaining network security is to monitor and manage all current and former employee access credentials and log all privileged account access activity to watch for unusual patterns of access behavior. When an employee exits the business, all passwords credentials, and authentications should be changed.



The Mobile Workforce

Mobile workers are part of today's organizational fabric. To maximize productivity, they use laptops, netbooks, tablet, and smart phones, to remotely access company applications and data. These devices are difficult to control and present several risks to the corporate network, systems, and data, as mobile devices can easily be lost or stolen. Working outside the office, from home, an airport, a hotel—anywhere there is a public Internet connection—presents a risk to corporate data because public and personal WiFi networks are not always secure. Building a secure infrastructure for a mobile workforce is essential and requires planning and policies. The plan must include a clear and detailed BYOD (Bring Your Own Device) policy and employees must be educated on all BYOD, mobile, and internal policies. Lastly, all remote users should have management software loaded on their mobile devices for monitoring and protection that can, for example, allow IT to remotely erase or lock a stolen or lost device.

Outdated and Unauthorized Software Use

Outdated software is an extremely common security problem. Cybercriminals work around the clock trolling for security holes to create increasingly sophisticated new viruses and malware. As a result, vendors of security software, applications, operating systems, and customized software regularly update their products to combat cybercriminals. It is critically important to corporate security that both enterprise software and user application software is up-to-date with all new patches and versions that remedy security threats.

Unauthorized software downloads—are serious risk factors. By nature, users seek technology tools that help them accomplish their tasks. As such, the security or integrity of the tool source is not verified. This can open a pathway for cybercriminals to breach the organization's network and access data. Similarly, downloading pictures or documents from both known and unknown sources can weaken the security of the corporate network. Therefore a security plan must include policies regarding both corporate sanctioned applications and allowed activities (e.g. social media, gaming, etc.) for corporate, network connected, devices.

What can organizations do to protect themselves?

Start with a Plan

Constant technology infrastructure advances, end-user behavior, and the ever-expanding threat landscape have transformed organizational security planning and implementation. A security plan with strict policies that are regularly reviewed and updated is the place to begin. In addition, an organization's security plan is an evolving process to assure that new threats are mitigated before a security event occurs.

In order to formulate a security plan, organizations must understand the variety of attack vectors that threaten their safety on a daily basis. Their plan must encompass regular security training, strict adherence to security policies and procedures, as well as effective methods of addressing the attack vectors of concern. This plan must also be updated and maintained regularly, as the threat landscape is always changing.

How do you add an additional layer of protection?

Managed Security Services Provider

Organizations sometimes choose to augment their staff in order to add an additional layer of protection. Using a Managed Security Provider and Networking expert, who combines technology and cybersecurity expertise, as well as an understanding of the overall business impact is a great way to do this. Managed Security Services Providers provide outcome-based improvements that align to business strategy and reduce risk. In addition to strategy they also enable threat intelligence and predictive security intelligence that scales and adapts against new and emerging threats.

Conclusion

The risks of not having a security plan in place to an organization are high. Data breaches can cause damaging work disruption, law suits, or business failure. According to Ponemon Institute's *Cost of a Data Breach* study, the cost of a data breach is up 6.4% in 2018 and the average total cost is $3.86m.

Global Study at a Glance

- Average total cost of a data breach:
  $3.86 million
- Average total one-year cost increase:
  6.4%
- Likelihood of a recurring material breach over the next two years:
  27.9%
- Average cost per lost or stolen record:
  $148
- One-year increase in per capita cost:
  4.8%
- Average cost savings with an Incident Response team:
  $14 per record

Sources: Ponemon Institute's Cost of a Data Breach study

The best strategy for maintaining corporate security is to develop and implement a comprehensive plan, perform ongoing education for all employees on threats and best practices, and continually monitor device and network access behaviors. This will assure that your employees follow the rules and support the goals of your organization—rather than indirectly or directly assisting the efforts of cybercriminals.