engage@crossroadstech.net | www.crossroadstech.net
Phone: 1-888-548-3893 | Fax: 1-610-736-0272

IT'S IN THE NUMBERS: CYBER SECURITY A CONSTANT THREAT

Introduction

High-profile security and data breaches have refocused attention on security issues within the organization. Between 2014 and 2015, companies such as Home Depot, Sony, Target, Blue Cross Blue Shield and the U.S. Office of Personnel Management experienced record news breaking attacks, with executives and security personnel losing their jobs as a result. The average total cost of a breach in 2014 was $1.33 million, and has risen to $1.57 million in 2015, according to the Ponemon Institute.

Expectedly, rising concern about IT security within organizations has transpired and forced decision makers to re-evaluate their security perceptions and strategies. There are three main concerns when dealing with IT security: the growing quantity and intricacy of attacks, the challenge of managing the ever growing complexity of information security and the tall cost of data breaches.

Top Three Concerns

The growing quantity and intricacy of attacks.

The challenge of managing the ever growing complexity of information security.

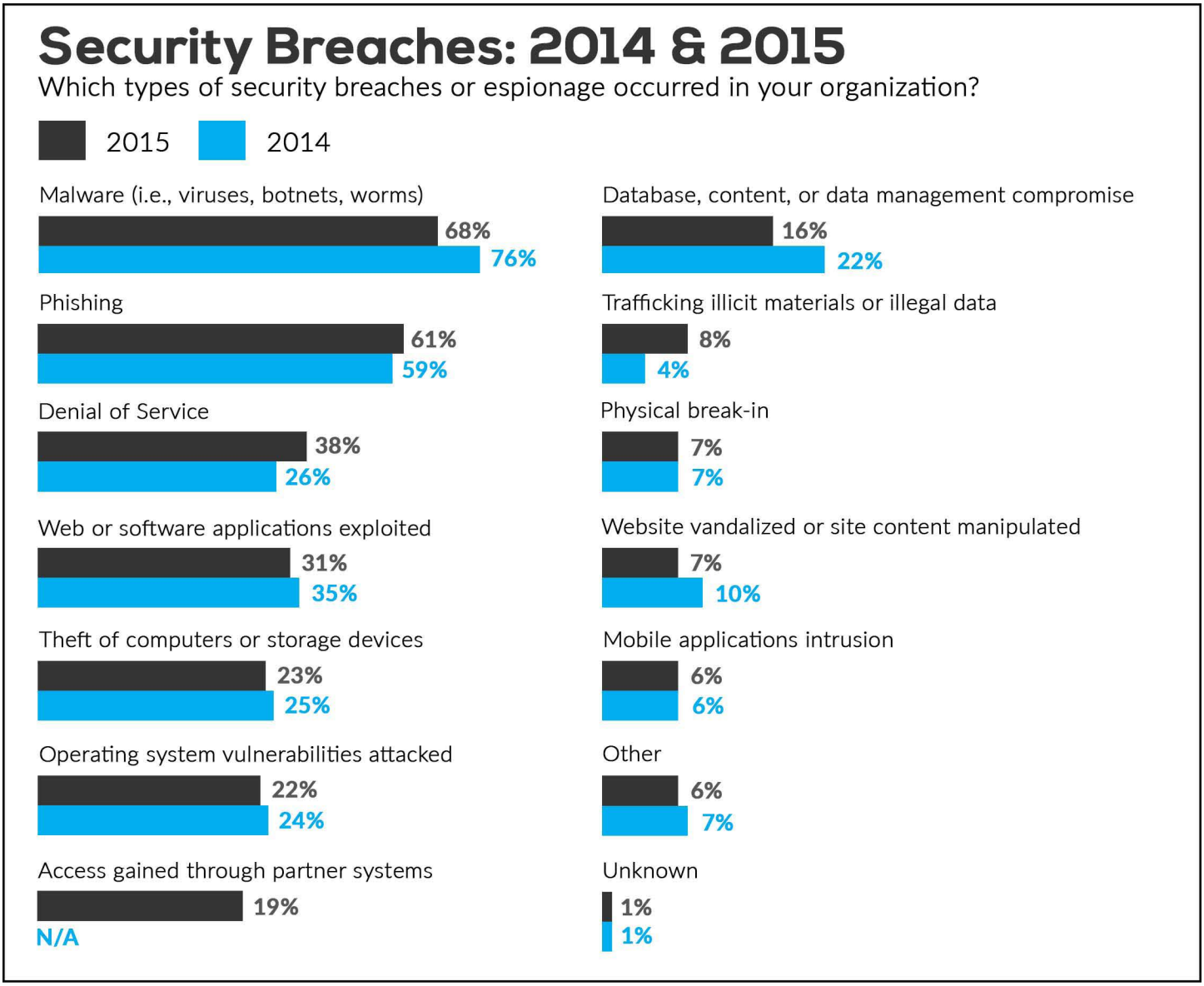
The tall cost of data breaches.

Table of Contents

Growing Quantity and Intricacy of Cyberattacks

A 2015 Strategic Security Survey, conducted by InformationWeek and Dark Reading, gathered information from 435 IT decision makers working in North American organizations. Through their study, they determined that certain types of IT attacks seem to be increasing: 61% of those surveyed reported phishing attacks within their organizations – up from 2014's 59% – and denial-of-service attacks increased from 26% to 38% in the same timeframe.

23% of respondents reported that their organizations had been compromised or breached as a result of cyber-attacks last year alone. 15% also said that they fell victim to attacks that were directly targeted at their organization. In a directly targeted breach, significant time and resources are invested by attackers. These direct attacks can be considerably more difficult to detect, prevent and diminish, and have more detrimental effects.



Note: Multiple responses allowed
Base: 101 respondents in April 2015 and 123 respondents in April 2014 who have experienced a security breach within the past year
Data: InformationWeek Strategic Security Survey of business technology and security professionals at organizations with 100+ employees

The Challenge of Complexity

According to IT decision makers, securing corporate networks is becoming more challenging and complex: when asked about their biggest information or network security challenges, 44% pointed to managing the complexity of security as a top concern.

Not only do the volume and intricacy of attacks add to the complexity of IT security, human behavior also appears to play a main role in the issue. Directly targeted attacks usually focus on staff, which is commonly a weak point in corporate security defenses.

As a result, respondents rated end-user security-awareness training as the most vital security practice in the workplace. Human behavior and, consequently, error, can be greatly reduced with some administration and oversight. Education regarding topics such as compliance, creating strong passwords, keeping devices safe and being aware of cyber threats can drastically reduce the possibility of internally caused breaches.

When asked about endpoint security concerns within their organizations, respondents were more concerned with the behavior of their employees than the level of security within devices and systems. Representing 58% of the survey group, the main concern with devices and systems involved connecting infected personal or company devices to organizational networks. Other common security threats amongst corporations included: users falling victim to phishing and other scams, as well as the loss of a device with sensitive or important information were also highly agreed upon as being detrimental to internal security efforts.

The Tall Cost of Breaches

Costs resulting from data breaches or compromises are often insurmountable. Though monetary losses can cost millions of dollars, it is not only finances that suffer post-attack. Physical damage can occur in system or hardware destruction, as well as other ways depending on the type of attack. Though this can be detrimental to an organization, non-physical damage can sometimes leave far bigger wounds.

When faced with major cyber-attacks, organizations are left defenseless, and sometimes scarred. Organizations can be consequently stuck with tainted reputations, loss of accountability and trust, compromised confidentiality and legal liability. While these factors may not have an immediate effect on an organization's finances, they may later when it comes to gaining new business.

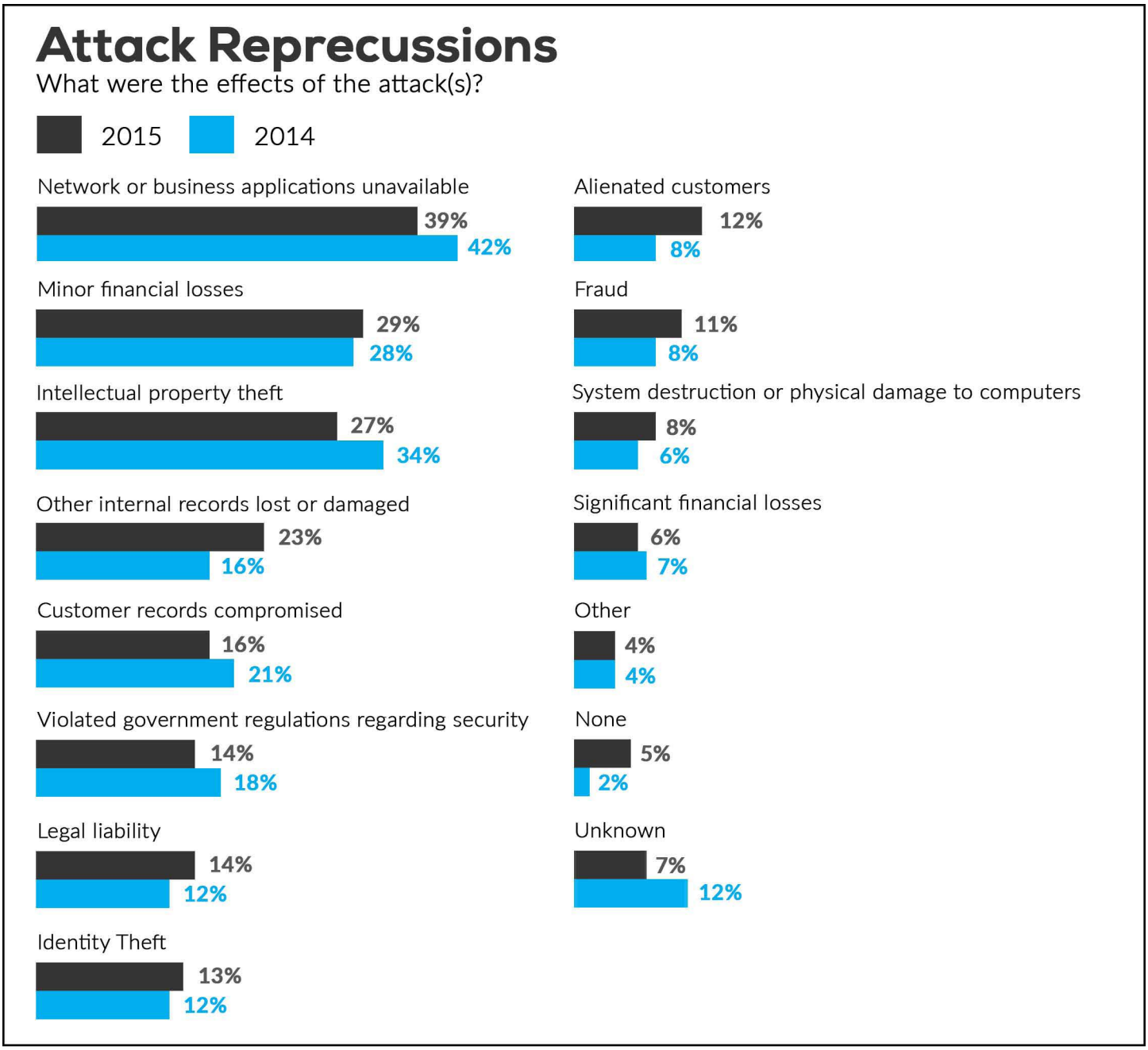
61%

of those surveyed said their organizations are becoming more vulnerable because of the increasing intricacy of attacks.

Effects on Organizations

Of those surveyed, 39% were unable to put a definitive price on how much their security breach had cost the organization. Of those who could, 32% said breaches had costed over $100,000, 12% said costs were over $1 million, and 6% said costs had exceeded $5 million.

In order to prevent as much damage and expense as possible, organizations are taking action by increasing security budgets. 46% of those surveyed expect their spending and defensive measures to increase this year. Most companies are left with no other choice in the matter, with the alternative to spending involving



Note: Multiple responses allowed
Base: 101 respondents in April 2015 and 123 respondents in April 2014 who have experienced a security breach within the past year
Data: InformationWeek Strategic Security Survey of business technology and security professionals at organizations with 100+ employees

possible breaches or compromises, which can result in the aforementioned damages to the company, as well as high costs, and possible employee terminations.

Countering Threats

Now is a very challenging time to be involved with IT security. Attackers are continuing to evolve and find new ways to inflict harm on organizational information and networks. It is imperative for companies to stay in touch with progressing security and defense mechanisms.

Finding a security partner who can help respond to the increasing quantity and intricacy of attacks is crucial. Organizations should look for a vendor with expertise in responding to threats, and who is always furthering their knowledge within the ever-changing security landscape. With this knowledge, as well as appropriate measures and strategies to manage security complexity, staff can easily navigate the increasing amount of threats that are faced. By leveraging these relationships, IT security can better defend organizations against increasing threats and data breaches.

How Do I Implement IT Security?

If you are interested in learning more about our security solutions, please contact one of our dedicated IT professionals at **888-548-3893** or **engage@crossroadstech.net**. We will happily provide you with an assessment of your current IT solution, and assist you in determining the best implementation route for your organization. Each professional is equipped to answer any and all questions on security that you may have, and would be grateful for an opportunity to assist you in advancing your business with proficiency, reliability, integrity, and accountability.

The Crossroads Difference

At Crossroads we work with forward-thinking organizations and understand the value of having the time and resources to gain a strategic advantage within their market segments. We have a proven track record, profound technological expertise and solutions that are innovative and successful.

Multi-Dimensional Solutions

Clients and organizations have the ability to not be partial to any segments of our abundant solution options. Choose solutions that best fit your organization and specifications, knowing that we take 100% accountability for everything you entrust with us.

100% Accountability

You will not find anyone else willing to take complete reliability for your IT, at whatever the cost. This is one of the critical anchor points of our engagements; we take full accountability for our engagements, and ensure that our solutions are solid and reliable at every level of the operational spectrum. We strive to provide clients with a seamless, transparent experience that will transform mission-critical challenges into stress-free moments.

Flat Communication

Our flat lines of communications will afford maximum proficiency in your workplace. We focus on providing zero-gap solutions that eliminate deficiency and provide single points of resolution. There is no tier climbing necessary to achieve desired results; our technicians are equipped to assist with any issue at any time and solve it successfully. We strive to produce exceptional results and customized solutions quickly.

Insightful Advice

You can depend on us to always proceed in your best interest, regardless of the circumstances. Through this firm foundation, we demonstrate integrity and reliability. We'll only offer expert professional assessments of how to best move forward in a given situation. The Crossroad's philosophy is that there's always a solution, and we'll be there to provide an expert honest assessment of the options at hand.

Experience

Crossroads has been in the business of providing for organizations since 1996; that's almost 20 years of experience aiding companies in IT and facilitating prosperity. We have molded our organization to constantly grow and adapt in technology, providing clients with the highest quality technological experience possible. We guarantee that our services will be successful, and take 100% accountability for them. If there is an error, we will be right there to rectify it or your money back.

engage@crossroadstech.net | www.crossroadstech.net
Phone: 1-888-548-3893 | Fax: 1-610-736-0272
3 Park Plaza, Wyomissing PA | 4141 S. Highland Drive, Salt Lake City UT