Website Security: Understanding the Challenges Modern Businesses Face

Author, Chris Tomlinson

A Peppersack White Paper

July 2015

---

www.peppersack.com

Website Security: Understanding the Challenges Modern Businesses Face by Chris Tomlinson

The Growing Prevalence of Attacks

Turn on the news, open the newspaper, or visit any online news outlet almost any day of the week and you'll see them – headlines proclaim yet another hack resulting in compromised data, business information, consumer financial records, medical information and more. Hacking is everywhere these days, and can take on a wide range of different forms. "Threats" is probably a more apt descriptor for what today's business owners and decision makers face, threats from a bewildering range of sources.

What's more is the fact that almost every website in existence is vulnerable, and through that website, your company's information. Whether you're involved in consumer healthcare, ecommerce, banking, R&D for the pharmaceutical industry or something else, you are vulnerable.

According to WhiteHat Security, 55% of retail and trade websites are always vulnerable, 50% of healthcare and social assistance sites are always vulnerable, and 35% of finance and insurance websites are always vulnerable. What does "always" mean, though? Simply put, it means these sites are vulnerable through serious security weaknesses every single day of the year. To top that off, 86% of websites in existence have at least one major vulnerability and multiple minor ones open to exploitation. 56% of websites have multiple serious vulnerabilities.

Given those numbers, chances are excellent that your website falls into the first category, and it's almost even odds that it falls into the second one as well. Note that this don't include the major high-profile ones, such as Heartbleed and ShellShock.

The most secure industry in terms of website protection seems to be educational services, where WhiteHat found 40% of sites were rarely vulnerable. Arts and entertainment sites came in just behind that with 39% of websites found to be rarely vulnerable.

With that being said, being part of these two industries doesn't guarantee protection. It doesn't mean your website is more secure. Rather, it simply means that those seeking to exploit vulnerabilities have been more engrossed with other industries because of a perceived higher payout (more valuable information, or data that can be more readily put to immediate use).

In an in-depth survey, WhiteHat found that 24% of respondents had suffered a data or system breach, with 17% of finance and insurance companies reporting these incidents and 20% of information related companies experiencing the same thing. Interestingly (and very telling), almost 60% of those respondents held no part of the organization accountable for breaches or loss of data.

However, the same study found that in organizations where accountability was high, remediation was 33%. For those without accountability, it was a dismal 24%.

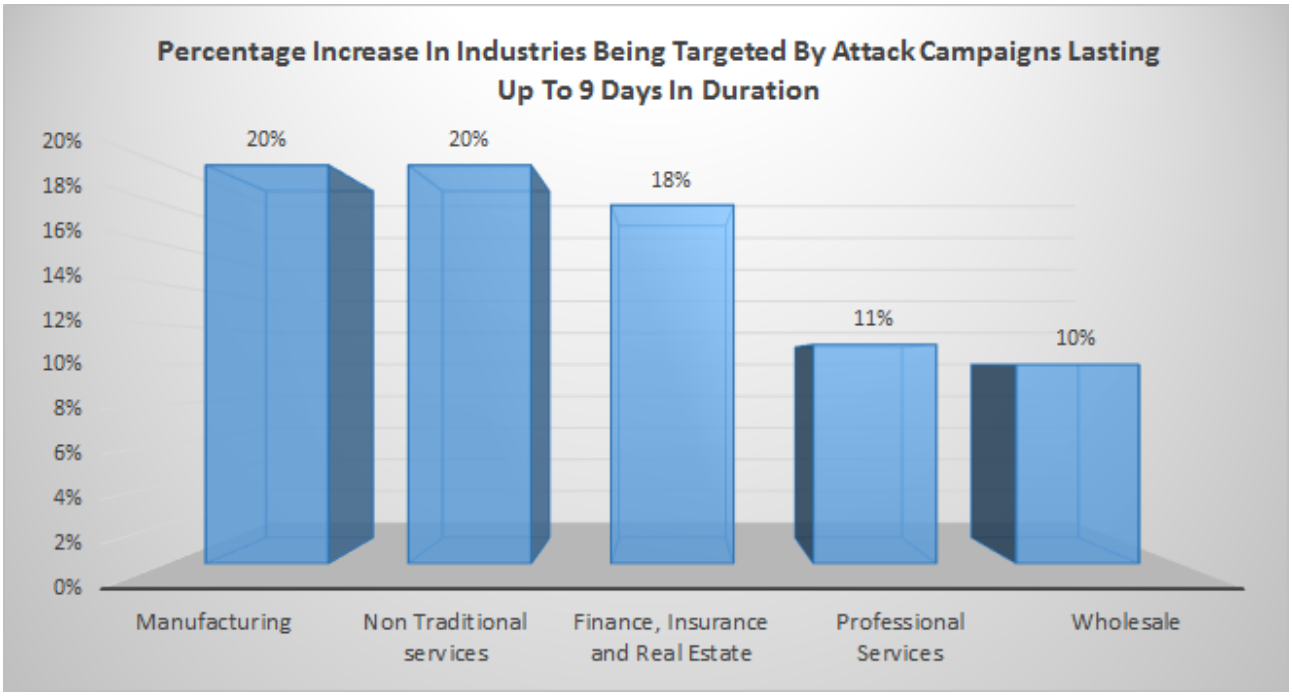
The Most Common Security Problems and Statistics

As mentioned 86% of websites contain at least one serious vulnerability, but what are those

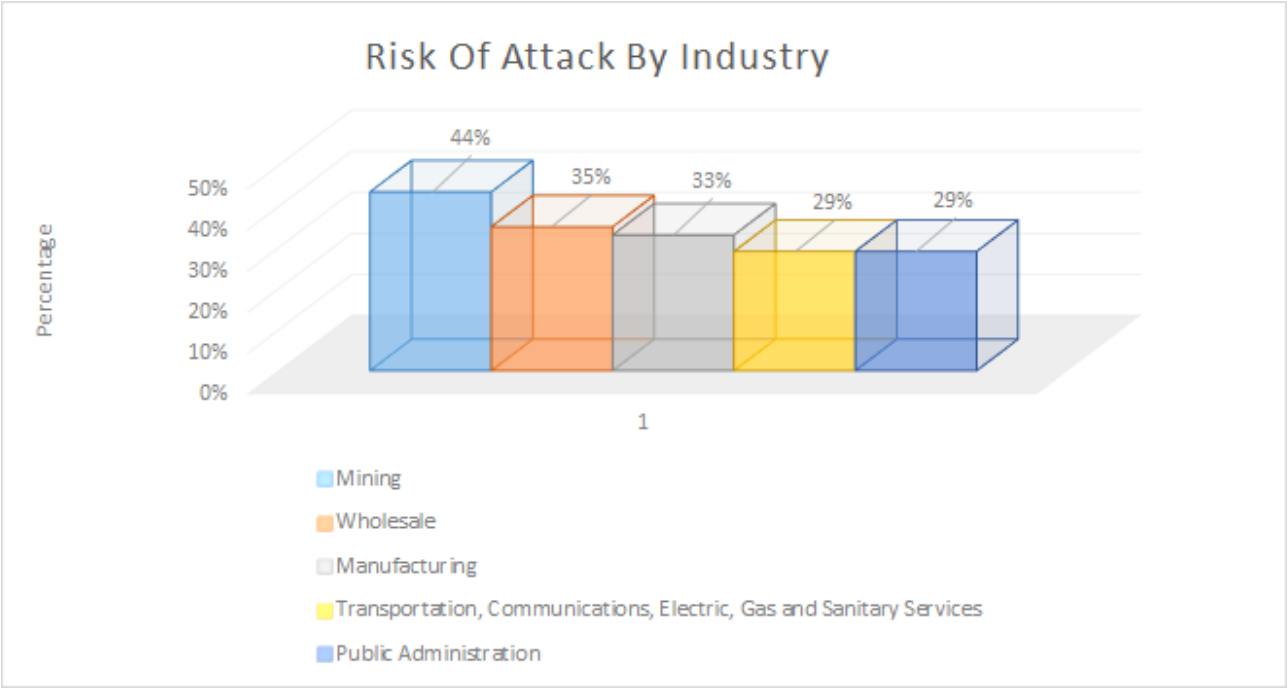
Peppersack Limited, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3670 Email: info@peppersack.com Web: www.peppersack.com
Registered in England and Wales 11th August 2009, Registered Number 6997254, VAT Number 981 3013 36

vulnerabilities and what sort of risk do they open your company up to? While the situation varies by industry, the most common problems can be found below:

- 70% insufficient transport layer protection/Retail/trade was the most affected, but information, finance, insurance and healthcare were included as well.
- 56% information leakage – Again, retail/trade was the hardest hit, with finance, insurance, information and healthcare coming in close behind.
- Other significant issues include cross-site scripting, SSL v2 (Secure Sockets Layer version 2) support detected, SSL weak cipher suites supported and invalid SSL certificate chains according to Symantec's annual security report.
- Only 61% of all security breaches were resolved.
- In those instances that were resolved, it required an average of 193 days.
- Companies/websites with few financially valuable network resources are more secure (less attractive targets).
- In 2014, 60% of attacks were directed at small or medium businesses, rather than large firms, so size is no protection.
- According to Symantec, 5 out of 6 large businesses were targeted with spear-phishing attacks in 2014, which marked a 40% increase over 2013. Similar attacks on small and medium businesses increased by 26% and 30%.
- 2014 saw the release of 317 million new pieces of malware.
- Symantec noted an increase in other industries being targeted by attack campaigns lasting up to 9 days in duration, which included (ranked from most growth to least):



Conversely, the company noted that the risk ratio for attacks was highest for the following (ranked by risk from highest to lowest):



- Manufacturing (20% increase)
- Nontraditional services (20% increase)
- Finance, insurance and real estate (18% increase)
- Professional services (11% increase)

- Wholesale (10% increase)

Conversely, the company noted that the risk ratio for attacks was highest for the following (ranked by risk from highest to lowest):

- Mining (risk ratio of 1 in 2.3)
- Wholesale (risk ratio of 1 in 2.9)
- Manufacturing (risk ratio of 1 in 3.0)
- Transportation, communications, electric, gas and sanitary services (risk ratio of 1 in 3.4)
- Public administration (government: risk ratio of 1 in 3.4)

A couple of examples pulled from recent headlines should show just how broad the spectrum of risk truly is (there's no such thing as an industry impervious to exploitation).

In May of 2015, the US Internal Revenue Service was targeted by what the AP called, "an elaborate scheme to claim fraudulent tax returns". The end result here was that 104,000 US taxpayers had their tax information stolen right from the government server. This was the result of significant effort on the part of organizations with plenty of resources, as well. An IRS spokesperson told reporters, "We're confident that these are not amateurs. These actually are organized crime syndicates that not only we, but everybody in the financial industry, are dealing with."

A few days later, the Portland Press out of Washington State, corroborated by Britain's Channel 4 news, reported that "the operator of a popular adult dating website said it's investigating a data security breach following reports that hackers stole names, email addresses and information about sexual orientation and habits of up to 4 million members." AdultFriendFinder.com was the target, and there is speculation (but no confirmation) that hackers also gained access to members' financial information.

However, not all exploits are targeted at gaining access to your database. Hackers can infiltrate your system and inject code to do any number of things from "defacing" your site to sending your visitors to a site of their choosing when they click on an innocuous link. Imagine the reaction of your customers when they attempt to make a purchase through your store, only to find themselves redirected to a completely different website.

It destroys trust, incites fear that their own computer or other device may have been compromised, and virtually guarantees they won't be visiting your website again. Perhaps the most insidious aspect of this is the damage done to your reputation – once tarnished, it may be impossible to ever rebuild trust with your audience.

What creates these vulnerabilities? The cause can range from internal to external, and includes bugs in software (poorly coded), employee password management practices, and the desirability of your company's information for those seeking to exploit vulnerabilities. Those businesses with the most valuable content are at the highest end of the spectrum in terms of risk, regardless of any other considerations. The more attractive your data is, the more incentive there is to breach your system.

Website Code and Web Security

Any website that allows users to interact creates potential vulnerabilities. This can include allowing your visitors to take any of a broad range of actions, from creating an account to searching for products or even just filling out a simple contact form. Any point of interaction can be turned into an exploit for a hacker or hacking software interested in gaining access to your system.

As noted by BeyondSecurity, in these instances “your web site visitor is effectively sending a command to or through your web server, very likely to a database. In each opportunity to communicate, such as a form field, search field or blog, correctly written code will allow only a very narrow range of commands or information types to pass in or out. This is ideal for web security. However, these limits are not automatic. It takes well trained programmers a good deal of time to write code that allows all expected data to pass and disallows all unexpected or potentially harmful data.”

Logically, the fewer features you have, the more secure your website. The most secure server is one that is barebones, with very few open ports and a limited number of services. However, that’s unlikely to be an option for most companies, particularly those seeking to use the web to foster growth and profitability.

For the vast majority of businesses, running a complex, multifunctional website requires multiple open ports, multiple services and more, which opens you up to a significant amount of risk. If your IT staff is diligent about patching and updating, you are at less of a risk, but you still have to contend with updates for the apps used, as well as for the website code itself.

In the company’s annual Internet Security Threat report, Symantec stated, “Web threats got bigger and much more aggressive in 2014 as holes in commonly used tools and encryption protocols were exposed and criminals made it harder to escape their malicious clutches. The web presented an incredibly threatening landscape in 2014, a trend set to continue in 2015. Vulnerabilities and new variants of malware underlined that website security deserves full-time, business-critical attention.”

The security giant noted that SSL / TLS (Transport Layer Security, TLS is SSL v3.1) vulnerabilities were the most visible threats in 2014 and moving into 2015. FREAK was added to the list of major threats that included Heartbleed and ShellShock, as well as Poodle (a lesser known but no less frightening attack). While Heartbleed might have garnered the most headlines, ShellShock was perhaps the most eye-opening for business owners simply because it occurred overnight. One day your servers and data were completely secure. The next day, they weren’t. That is exactly how quickly the Internet security landscape changes, and what your business must be prepared to address on an ongoing basis. You might be more familiar with the name BashBug than ShellsShock, but both names apply to the same thing. Web servers are the simplest route for an attacker using the CGI (Common Gateway Interface). Using this avenue, attackers would send a command to an environment variable. The server would interpret that variable and run it (because it contained the vulnerability). This was very different from the way Heartbleed worked.

Poodle was another excellent example of the myriad threats out there. This vulnerability would make it possible for attackers to exploit servers that supported older SSL protocols, particularly SSL 3.0, by interfering with the handshake process used for verifying the server’s protocol using only SSL 3.0 regardless of whether there was a newer one supported. This highlighted the need for better encryption such as upgrading RSA-2048 key (RSA are the initials of the inventors of the first practical public-key cryptosystem) to an ECC-256 key (Elliptic Curve Cryptography) which is estimated to be 10,000 more

difficult to hack. Followed by the need to introduce PFS (Perfect Forward Secrecy) a key-agreement protocol ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

Each of these vulnerabilities exposed different weaknesses in the system, but they all shared one commonality – the need to manage vulnerabilities on the business' end. Writing for Symantec, Tim Gallo stated, "Over the past few years, the idea of vulnerability management has been frequently talked about but was often seen as an annoyance or a process that, while interesting, isn't as important as breach response or adversary tracking. However, 2014 gave vivid examples of the importance of addressing vulnerabilities."

One of the most pertinent things about these three vulnerabilities (all of which have been addressed today), is the fact that they were discovered in areas that weren't traditionally covered by vulnerability management processes. Because most major PC and laptop software manufacturers (think Microsoft, Apple and Adobe) have upped their game in terms of patch frequency and urgency, attackers have had to change their tactics.

The differences with ShellShock should be used as an example of what will come in 2015, 2016 and beyond. It relied on a vulnerability that existed for 25 years without being discovered and addressed. The fact that it was a Linux/UNIX/Mac OS exploit meant that it pertained to almost every single type of server on the web, from routers and Linux servers to email servers and more – anything that used Bash (Bash is a Unix shell and command language written by Brian Fox for the GNU Project as a free software replacement for the Bourne shell). This is the way of the future. Attackers will continue to comb through software looking for vulnerabilities and flaws to exploit. Things that were thought secure will be found to be lacking, and new threats will explode overnight.

Malware and Web Attack Toolkits

Malware and web attack toolkits take advantage of the fact that all too often, those responsible for maintaining software lack the time or inclination to apply patches and updates immediately. Given the number of patches for some programs, it can be a daunting prospect. This allows malware developers to exploit weaknesses that would otherwise be eliminated.

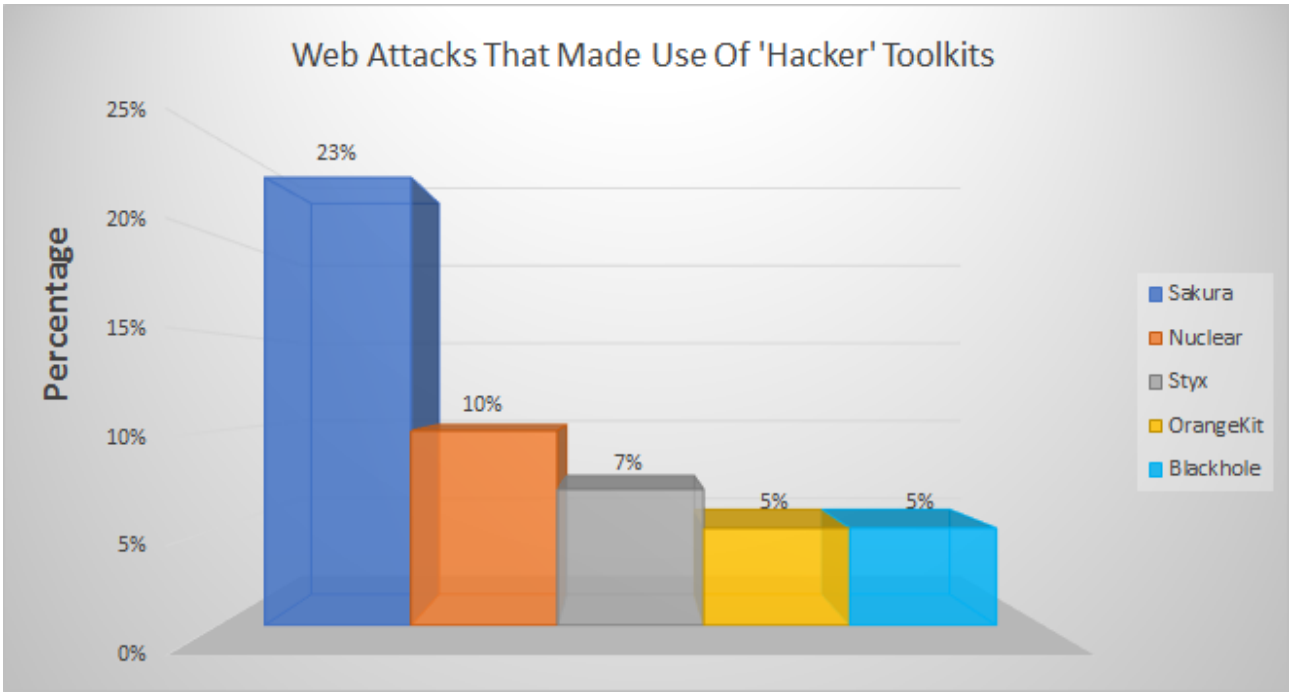
With malware, the situation is explained by Symantec as "a specialist 'dropper' scans for a number of known vulnerabilities and uses any unpatched security weakness as a back door to install malware." Web attack toolkits have made things simpler for attackers, as well. These toolkits do most of the work on the attacker's behalf, scanning and identifying areas ripe for exploitation, and then even suggesting the type of attack that will have the most/best results.

A significant number of websites are infected with malware (1 in 1,126), and these infected sites were responsible for an increased number of attacks in 2014 and early 2015. This is largely thanks to the ever-more popular SaaS concept. Some web attack toolkits are designed as software as a service (SaaS) and can be used in the cloud.

Here's an example of how such an attack would work, as explained by Symantec. "A compromised website may use an HTML iframe tag (The <iframe> tag specifies an inline frame. An inline frame is used to embed another document within the current HTML document.), or some obfuscated JavaScript in order to inject malicious code from the SaaS-based (Software-as-a-Service) exploit toolkit rather than launch the

malicious attack directly from exploit code hosted on the compromised website. This growth in SaaS-based exploit toolkits is also evidenced in the decline in the number of new malicious domains used to host malware, which fell by 47% from 56,158 in 2013 to 29,297 in 2014."

As an example of just how prevalent these toolkits have become, here are just the top five and their prevalence in use by attackers:



- Sakura (23% of all attacks)
- Nuclear (10% of all attacks)
- Styx (7% of all attacks)
- OrangeKit (5% of all attacks)
- Blackhole (5% of all attacks)

The remaining 50% of attacks were carried out using other types of kits, of which there is a staggering array, none of which has more than 5% of the total. It's also important to note that these toolkits change regularly. For instance, Blackhole made up 41% of the total of attacks in 2013, but fell to 5% in 2014 due to the creator's arrest. Other toolkits rose to take its spot, and this cycle will continue, with new kits being developed all the time.

Targeted Attacks

It's important to note that the vast majority of attacks on websites are not targeted at that specific site alone. Most compromised sites are the result of blanket attacks, where hackers aren't particular about which sites they ultimately compromise. However, the incidence of targeted attacks is on the rise, with cyberespionage seeing one of the most significant increase in 2014 and early 2015. There are several

different types of targeted attack. These include:

- Direct hackers
- Competitors
- State-sponsored cyberespionage

Of all these types, direct hacking by individuals is becoming less common. This is due to a number of factors. Most hackers today are using more sophisticated methods of gaining access to the systems they target. No longer are they limited to amateurish tools and methods. In fact, there are entire business models built on the hacker-for-hire model, and the software utilized by these groups is incredibly sophisticated.

Targeted attacks can be carried out by any number of individuals or organizations. The list of potential threats has grown considerably just in the last year or two (and more will undoubtedly be added in the future). Today, the list of potential hackers/hacking groups includes the following:

- State-sponsored hackers and hacking organizations
- Data thieves
- Criminal extortionists
- Patriotic hackers
- Hacktivists

While these individuals and groups certainly use email attacks (spear-phishing, for instance, which we'll cover in the next section), a growing number are utilizing highly advanced web-based attacks. For instance, espionage attacks now bundle exploits together, rather than pursuing one at a time, granting access to systems much more quickly than would otherwise be possible.

One of the best examples of this type of software is Reign. Incredibly complex and powerful, Reign gave users the ability to spy on entire governments, the telecom industry, businesses, researchers and more. The software required five stealth installation steps and featured a modular design so that users could pick and choose the features they needed most. The software's capabilities ranged from password theft to screenshots to remote access, monitoring of network traffic, and even recovery of deleted files. That should be frightening. What's even more frightening is the fact that Reign was most likely created by a nation state, as it took years and a significant amount of funding to develop.

Other similar campaigns have included Dragonfly, Turla and Waterbug, all of which share marked similarities in terms of scope and cost, and suggesting that most if not all were created at the behest of some national government. Additionally, hackers are increasingly targeting non-traditional elements. For instance, one area that has seen significantly increased targeted attack frequency is industrial control systems, or ICSs. These include industrial production and manufacturing, but also include utility services and the like.

Preeti Agarwal explains the situation as, “Targeted attacks have evolved from novice intrusion attempts to become an essential weapon in cyberespionage. Industrial control systems are prime targets for these attackers, with motives for executing attacks at a national security level. These trends are leading countries to reinforce their investment and build strategies to improve ICS security.”

She goes on to explain a concept that applies to all businesses with a website or Internet connected technology. “Many of the proprietary web applications have security vulnerabilities that allow buffer overflows, SQL injection or cross-site scripting attacks. Poor authentication and authorization techniques can lead the attacker to gain access to critical functionalities. Weak authentication allows for man-in-the-middle attacks like packet repay and spoofing.”

Spear-Phishing: A New Twist on an Old Threat

Unless you’ve been living under that proverbial rock, you’ve at least heard of phishing, and there’s an excellent chance that you or your employees have received one or more phishing emails. While phishing might be on the way out, there’s a new twist on this old threat, and it’s posing a significant problem for businesses large and small. In fact, size is no protection against this form of hacking, and attackers are actually almost as likely to target a small company as they are a large one.

In 2014, 34% of all spear-phishing attacks were targeted at small businesses. 41% of attacks were against large companies. Only 25% were made against medium sized firms.

What is spear-phishing, though? As mentioned, it’s an evolution of the older phishing technique, and it relies on email and user susceptibility to succeed. It can be used against businesses, organizations, government agencies and individuals, and it relies on familiarity to work.

Kaspersky explains it as, “Spear-phishing is a targeted email scam with the sole purpose of obtaining unauthorized access to sensitive data. Unlike phishing scams, which cast broad, scatter-shot attacks, spear-phishing hones in on a specific group or organization. The intent is to steal intellectual property, financial data, trade or military secrets and other confidential data.”

Make note of those goals – you’ll notice they’re much more oriented on businesses and organizations than on individuals (although individuals are targeted, particularly to gain access to an organization or business where they are employed). This method has been responsible for some very high profile breaches, including the compromising of a server at JPMorgan Chase. The Information Security Media Group reports that, “Hackers are increasingly focusing their phishing campaigns against bank employees rather than bank customers. Instead of going after thousands of customers, they are going after the bank itself and they are finding that they are really successful.”

Here is how a spear-phishing attack might occur. An employee comes to work one morning and turns on his or her workstation. After it boots up, the employee opens the email program (or accesses a web or network-based email platform). In the inbox is a message from someone the employee knows. It might be another employee, a supervisor or even a vendor with which the company works. The employee opens the message, is assured that the sender is valid thanks to correct information and a personal tone, and clicks the link within the email. Once they do this, their credentials are compromised, and the hacker has access to every level of the system to which that employee is authorized.

Norton explains the process as, “The spear phisher thrives on familiarity. He knows your name, your email address and at least a little about you. The salutation on the email message is likely to be personalized: ‘Hi Bob’ instead of ‘Dear Sir’. The email may make reference to a mutual friend or to a recent online purchase. Because the email seems to come from someone you know, you may be less vigilant and give them the information they ask for. When it’s a company you know asking for urgent action, you may be tempted to act before thinking.”

The Information Security Media Group expands on this. “These targeted emails can appear to be coming from other management or staff within the institution itself, asking the employee to provide urgent information about an account or a system. Or, sometimes they can appear to come from outside sources, such as a vendor or even a customer.”

Kaspersky explains, “Many times, government-sponsored hackers and hacktivists are behind these attacks. Cybercriminals do the same with the intention to resell confidential data to governments and private companies. These cybercriminals employ individually designed approaches and social engineering techniques to effectively personalize messages and websites. As a result, even high-ranking targets within organizations, like top executives, can find themselves opening emails they thought were safe. That slip-up enables cybercriminals to steal the data they need in order to attack their networks.”

The most frequently targeted individuals within an organization for spear-phishing attacks have been identified by Symantec as follows:

- Sales and Marketing (1 in 2.9, or 35%)
- Finance (1 in 3.3, or 30%)
- Operations (1 in 3.8, or 27%)
- R&D (1 in 4.4, or 23%)
- IT (1 in 5.4, or 19%)
- Engineering (1 in 6.4, or 16%)
- HR and Recruitment (1 in 7.2, or 14%)
- Other (1 in 9.3, or 11%)

Most of these emails contain a file, with the most common being .doc. However, .exe, .scr, .au3, .jpg, .class, .pdf, .bin, .txt and .dmp are also used.

The challenge inherent with defeating spear-phishing attacks is that it cannot be done solely through the use of software and ensuring that patches and updates are applied regularly. It requires a significant commitment on your company’s part to employee education and training. Awareness is the key to ensuring that these email attacks are not successful and your systems remains secure.

Data Breaches

The most frequently talked about events and those most frequently seen in the headlines are data breaches. While they're far less common than spear-phishing or other attacks, data breaches have the potential to be devastating, for both the business or organization, and their customers, clients, vendors and other associated parties.

The number of mega-breaches dropped in 2014, but the number of total breaches actually jumped by 23%. Of these, 49% were caused by hackers. Other causes include data leaks, lost devices, employee error and more.

While there are numerous potential weak points through which an attacker might penetrate a system, individual accounts remain the most common access point. For instance, take the Apple iCloud breach that exposed almost 200 celebrity photographs as an example. This hack was very widely reported, with the pictures (mostly nudes) being distributed on 4chan and other online sites. However, according to Apple, the problem was not with security at their end. Rather, the breach was the result of "highly tailored targeted attacks on individual accounts".

Additionally, the range of industries targeted by hackers is changing. Healthcare has long led the pack, and 2014 was no different, with this sector making up 37% of the total of hacking incidents in the entire country. This was the fourth consecutive year that healthcare businesses were so frequently targeted. Following healthcare was the retail sector, with 11% of the total. Education accounted for 10%, while government and public organizations were targeted 8% of the time. Financial businesses were attacked 6% of the time, and computer software developers saw 4% of the total. The hospitality and insurance sectors were likewise at 4%, while transportation and arts/media were under that mark.

With that being said, the greatest devastation in terms of identities exposed was in the retail sector, with 59% of all the identities exposed. The financial sector came in second, with computer software, healthcare, government, social networking, telecom, hospitality, education and arts/media following in that order.

The Importance of Responsibility in the Face of Security Breaches

As mentioned previously in this report, the number of organizations and businesses with a clear chain of responsibility in the face of security breaches is dismally low. Among those with solid responsibility plans, remediation is much more likely to be successful, and breaches are less frequent. Those lacking responsibility chains are less likely to see successful remediation, and more likely to be targeted or victimized in the first place.

According to WhiteHat Security, there are few "best practices" that are applicable to every business and organization. Among those that are is the need for clearly delineated responsibility. To whom do you turn when a breach has occurred? Who is responsible for patching and updates? Who is responsible for remediation? It is vital that your business or organization have a specific, tailored set of metrics in place for responsibility.

It is also essential that your organization be able to communicate clearly when it comes to compliance, goals, ad hoc code reviews and a great deal more. The following checklist can help foster better communication and transparency, while providing the means to enhance security for systems and

websites:

- Has automatic static analysis been incorporated into the code review process?
- How frequently are security reviews conducted, and where are those results sent?
- How often is adversarial testing performed?
- How often and when does penetration testing occur?
- What is our incidence response plan?
- When was it last updated?
- What is the responsibility chain for breaches and other incidents?
- When are security-focused design reviews of web applications performed?
- Do we maintain a list of the most important bugs to be fixed?
- How and when are patches and updates applied? Whom is responsible for updating and patching?
- What is our stance/position on employee education regarding spear-phishing attacks?
- Are website configuration files hidden properly?
- Is antivirus protection available for the website?
- Are all unused/outdated user accounts deleted regularly?
- Are unused/unnecessary databases and applications deleted regularly?
- Is access control implemented? Is our access control solution role-based?
- Is our SSL always on?
- Are we utilizing ECC-256 key security?
- Have we implemented Perfect Forward Secrecy?

Summary: The Risk Is Not Insurmountable

While 2014 and early 2015 saw increases in security risks, breaches and attacks, the risk to businesses and organizations is not insurmountable. Combining the right tactics with robust software and a clear-cut chain of responsibility with employee education and awareness will enhance your ability to defeat attacks and stay out of attackers' crosshairs in the first place.

While there is no single industry immune to website hacking and security risks, organizations can take steps to drastically reduce the amount of risk to which they are exposed. Attackers are becoming more resourceful, more patient, and more sophisticated. As Symantec notes, good security processes and

implementations are all that stand in the way of total financial and reputational ruin. Take the steps necessary to protect your business and its assets.

The steps to take are clear:

Get stronger SSL. Upgrading your SSL is essential, considering this is one of the primary avenues for attack. Even Microsoft and Google have announced that SHA-1 will be depreciated in favor of more secure SHA-2.

Improve your security. If you're still using the industry standard RSA-2048 key, it is essential to move to an ECC-256 key, which is reportedly 10,000 times more difficult to hack. Hackers are forced to spend more time and effort in these instances, and will likely move on to less protected targets instead.

Introduce PFS (Perfect Forward Secrecy) which works much better with ECC-256 key security than with RSA encryption. With PFS, even if a hacker were to steal your SSL certificate private keys, they cannot decrypt any historical information.

When it comes to SSL, it's essential that you take several steps. It should always be on. Your servers should always be up to date. Your website should display recognized trust marks (Norton or Kaspersky logos, for instance). Scan your website regularly, but do not stick to a specific schedule. Ongoing, random scans can help prevent vulnerabilities and malware from compromising your site.

Ensure that your server configuration is up to date. Old SSL versions must be disabled, and new versions enabled and prioritized correctly.

Finally educate your employees on good security habits. These are "old hat", but they bear repeating. Never open an attachment from an unknown sender, and even if the sender is known, think twice about opening any executable. Two-step authentication should be adopted on any device that will permit it, from email accounts to smartphones and laptops.

Protecting your business from hackers is a tall order, but it can be done. Two of the most important areas of concern for small, medium and even large services are SaaS solutions and web apps. Both must be constantly monitored and updated. Moreover, code should be custom developed to meet specific business requirement, never reused (which is what led to issues like Heartbleed and ShellShock). At Peppersack, these are two of our core competencies, and we ensure that our SaaS offerings and web apps are always 100% monitored and up to date.

Works Cited:

http://www.beyondsecurity.com/web-security-and-web-scanning.html
http://www.symantec.com/security_response/publications/threatreport.jsp
http://www.scmagazine.com/whitehat-security-release-website-security-statistics-report/article/416402/
https://www.whitehatsec.com/press-releases/featured/2015/05/21/pressrelease.html
https://www.whitehatsec.com/statistics-report/featured/2015/05/21/statsreport.html
http://www.mb.com.ph/security-breach-104000-taxpayers-have-personal-info-stolen-from-irs-website/
http://www.pressherald.com/2015/05/23/adult-dating-website-investigates-possible-security-breach/
https://usa.kaspersky.com/internet-security-center/definitions/spear-phishing#.VWb8n1VVhBc

Peppersack Limited, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3670 Email: info@peppersack.com Web: www.peppersack.com

Registered in England and Wales 11th August 2009, Registered Number 6997254, VAT Number 981 3013 36

http://www.bankinfosecurity.com/spear-phishing-bigger-concern-in-2015-a-7742/op-1

Peppersack Limited, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3670 Email: info@peppersack.com Web: www.peppersack.com
Registered in England and Wales 11th August 2009, Registered Number 6997254, VAT Number 981 3013 36

About Peppersack

Peppersack is a leading digital marketing agency providing SEO and content marketing services that deliver results. Our search engine optimisation services will help to raise your page rank. We deliver proven results in the form of traffic to websites and sales inquiries though integrated inbound marketing campaigns. We make it easy for your potential clients to find you. These services are based on a disciplined approach to research, analysis, business planning and reporting. Support services include content development, social media management and creative design and development.

Contact Peppersack

Please contact us for help and advice with your digital marketing and communications

Email: contact@peppersack.com
Telephone: 0161 926 3670
Atlantic Business Centre
Atlantic Street
Manchester
WA14 5NQ
web: www.peppersack.com