PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions
August 2021

Did You Know?

Did you know that the #1 priority for corporations is keeping their information secure? According to a recent survey from Forrester Research, companies are not putting enough focus on their network **and the threat of a potential cybersecurity breach is greater than ever before.** As a result, many businesses are looking for solutions to protect themselves better. One such solution is using a self-paced autonomous AI endpoint security platform like **SentinelOne.**

SentinelOne is designed **to protect enterprises from ransomware and other malware threats**. It recognizes the behaviors of ransomware and prevents it from encrypting files. Additionally, it is able to rollback Windows devices in the event that files are encrypted. **Call us at 561-969-1616 to learn more!**

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Phishing Costs Nearly Quadrupled Over 6 Years

Research shows that the cost of phishing attacks has nearly quadrupled over the past six years: Large U.S. companies are now losing, on average, $14.8 million annually, or $1,500 per employee.

That's up sharply from 2015's figure of $3.8 million, according to a new study from Ponemon Institute.

According to the study, **phishing leads to some of the costliest cyberattacks.**

One of the most expensive threat types is business email compromise (BEC). BEC costs ramped up significantly in 2020, with more than $1.8 billion stolen from organizations as cybercrooks launch ever slicker attacks, either impersonating someone inside an organization or masquerading as a partner or vendor in order to pull off financial scams.

Another one of the most expensive attacks is **ransomware**, as experts have tracked exploding ransom costs.

But what businesses shell out for extortion payments in ransomware attacks or what gets jimmied out of them in fraudulent BEC wire transfers are both ***just portions*** of the true costs of phishing attacks, according to the study, titled **The 2021 Cost of Phishing**.

"When people learn that an organization paid millions to resolve a ransomware issue, they assume that fixing it cost the company just the ransom. What we found is that ransoms alone account for less than 20 percent of the cost of a ransomware attack," said Larry Ponemon, chairman and founder of Ponemon Institute, in a press release. "Because phishing attacks increase the likelihood of a data breach and business disruption, most of the costs incurred by companies come from lost productivity and remediation of the issue rather than the actual ransom paid to the attackers."

Lost Productivity is the Biggest Gotcha

It's the lost productivity and mopping up that eat up the lion's share of the costs of phishing attacks, with a host of other investigative and compliance costs in the mix. Research has shown that the most

continued on page 2

time-consuming tasks to resolve phishing scams are the cleaning and fixing of infected systems along with conducting forensic investigations.

The study found that in an average-sized U.S. corporation of 9,567 people, that lost productivity translates to 63,343 wasted hours every year. Each employee wastes an average of 7 hours annually due to phishing scams: an increase from 4 hours in 2015.

The study, initially conducted in 2015, surveyed nearly 600 IT and IT security practitioners.

Researchers found that the average annual cost of phishing has increased from $3.8 million in 2015 to $14.83 million in 2021. The study showed productivity losses have spiked, from $1.8 million in FY2015 to $3.2 million in FY2021. (Information about BEC and ransomware wasn't available in FY2015.) In this, the most current study, annual cost of phishing for BEC was estimated to be $5.97 million, while average ransomware costs were estimated to total $996,000.

The BEC Blues

Some of the study's key takeaways:

- BEC costs nearly $6 million annually for a large organization. Of that, illicit payments made annually to BEC attackers is $1.17 million.
- Ransomware annually costs large organizations $5.66 million. Of that, only $790,000 accounts for the paid ransoms themselves.
- Security awareness training reduces phishing expenses by more than 50 percent on average.
- Costs for resolving malware infections have more than doubled since 2015. The average total cost to resolve malware attacks is $807,506 in 2021, an increase from $338,098 in 2015.
- Credential compromise costs have increased dramatically since 2015. As a result, organizations are spending more to respond. The average cost to contain phishing-based credential compromises increased from $381,920 in 2015 to $692,531 in 2021. Organizations experienced an average of 5.3 compromises over a 12-month period.
- Business leaders should pay attention to probable maximum loss scenarios. For instance, BEC attacks could incur losses from business disruptions of up to $157 million if organizations aren't prepared. Malware resulting in data exfiltration could cost businesses up to $137 million.

The cost of credential compromise has skyrocketed in recent years due to threat actors targeting employees instead of networks. It leaves the door wide open for much more devastating attacks like BEC and ransomware.

These attacks will continue to increase until organizations deploy a "staff-centric" approach to cybersecurity that includes security awareness training and integrated threat protection to stop and remediate threats.

Is your business protected? **Contact us for a complimentary cybersecurity assessment that will uncover any vulnerabilities that exist.** In addition, PalmTech offers Cybersecurity Training that will educate employees so they can recognize threats and take the proper action, which is a great step towards creating a stronger cybersecurity culture within your workplace.

Call us at 561-969-1616 for details to ensure your staff and your organization are protected or visit:

www.palmtech.net/cyber-security-assessment/

Hackers dedicate time EVERY week to keeping up with security news, trends, and technologies
Are your employees doing the same to stay one step ahead?
Call us about Security Awareness Training for your staff! (561)969-1616

Ransomware Hits Law Firm Counseling Fortune 500, Global 500 Companies

Campbell Conroy & O'Neil, P.C. (Campbell), a US law firm counseling dozens of Fortune 500 and Global 500 companies, disclosed a data breach following a February 2021 ransomware attack.

Campbell's client list includes high-profile companies from various industry sectors, including automotive, aviation, energy, insurance, pharmaceutical, retail, hospitality, and transportation.

Some of its current and past clients include Exxon, Apple, Mercedes Benz, Boeing, Home Depot, British Airways, Dow Chemical, Allianz Insurance, Universal Health Services, Marriott International, Johnson & Johnson, Pfizer, Time Warner, and many others.

Ransomware attack leads to data theft

"On February 27, 2021, Campbell became aware of unusual activity on its network," the law firm revealed in a press release issued last month.

"Campbell conducted an investigation and determined that the network was impacted by ransomware, which prevented access to certain files on the system."

The company hired third-party forensic investigators to investigate the incident after discovering the attack and notified the FBI of the security breach.

Campbell issued a press release providing notice because the investigation determined that information relating to affected individuals was accessed by the threat actors behind the ransomware attack.

While no clear evidence of the ransomware operators accessing specific information for each potentially impacted individual, Campbell confirmed that the affected devices contained various data types.

As Campbell found, the attackers were able to access "certain individuals' names, dates of birth, driver's license numbers / state identification numbers, financial account information, Social Security numbers, passport numbers, payment card information, medical information, health insurance information, biometric data, and/or online account credentials (i.e. usernames and passwords)."

Campbell offered 24 months of free access to credit monitoring, fraud consultation, and identity theft restoration services to all individuals whose Social Security numbers or equivalent information was exposed during the attack.

Incident could lead to additional data breaches

Campbell didn't reveal the identity of the ransomware group behind this attack or if the attackers stole the accessed data.

However, over 20 different ransomware operations are known to steal sensitive files from victims' servers before deploying payloads and encrypting their victims' devices.

The data stolen in these attacks is commonly used as leverage to force victims to pay ransoms under the threat of having their information gradually leaked online until the ransomware operators' demands are met.

Furthermore, in some cases, the ransomware gangs are also increasing the ransom bit-by-bit until all the stolen files are leaked on sites specifically designed for this purpose.

Depending on and if corporate clients' data was also stolen during the ransomware attack on Campbell's network, the incident could lead to more data breaches reported in the coming weeks and months.

Ransomware has abruptly grown as a threat reaching exceptional levels during the last few months, since the start of 2021.

Attacks have hit US business and critical infrastructure, including the world's largest meat producer JBS Foods and the largest US fuel pipeline Colonial Pipeline.

More recently, REvil ransomware breached Miami-based MSP software provider Kaseya in a campaign that hit roughly 1,500 businesses worldwide.

Are you confident that your firm or business is protected from cyber attacks? Don't wait to find out the hard way...

Is Your Firm or Business Protected From Cyber Attacks?

! For a limited time, PalmTech is offering a !

Free And Confidential Cyber Security Risk Assessment, Normally Valued at $1200, That Will Reveal Where Your Company Is At High Risk To Ransomware, Hackers And Other Devastating Cyber Attacks.

For Detail, Visit:

www.palmtech.net/cyber-security-assessment/

How Co–Managed IT Could Save Your Company From Financial Disaster

When you consider the investments in your business that you can make as a CEO, you probably think to yourself, "Which investments will give my company the best ROI?" With that in mind, would you think of making a significant investment in bolstering your IT department?

Many CEOs are understandably hesitant to throw a lot of money into their IT department because the ROI is more difficult to estimate. That said, though, consistently updating your company's IT services is becoming increasingly crucial to the continued success, and indeed safety, of your company. Ransomware and other cyber-attacks that steal company data are becoming more frequent and more costly, while IT departments continually get the short end of the budgetary stick.

While that all undoubtedly sounds horrible, you might be wondering just what you can do about it. After all, you only have so much money you can invest back into your company's IT department, and it might not be sufficient for keeping your IT staff from getting burned out, disgruntled or making costly mistakes - even when they're performing their responsibilities to the best of their abilities.

What if there were a way that you could have access to the most up-to-date IT knowledge and software while also not having to shell out the funds necessary to update your systems and hire more knowledgeable employees? Well, that's where co-managed IT can be your company's life preserver.

Co-managed IT is a flexible system for keeping data for your company, employees and clients safe from cyber-attacks as well as assisting in your daily operations where needed. Think of it as "filling in the gaps" that your current IT department (try as they might) struggle to fill.

For instance, say your current IT department is great at taking care of the day-to-day fires that inevitably come up in a normal workday, but they struggle to get to the "important but not urgent" task of updating your company's cyber security and creating data backups. Maybe it's the other way around, where your IT department is very focused on security, but they struggle to find time to assist employees with password resets and buggy programs. Maybe neither of these cases describes your IT department, but they still need better access to the tools and software that would allow them to reach their full potential in protecting the company's sensitive information. Or maybe your company is going through a period of rapid expansion, and you just don't have time to build the kind of IT infrastructure that would best serve your needs.

Regardless of what your IT department's current needs are, co-managed IT is the solution. We're here to do the tasks and provide the tools that your current IT department just can't provide. Make no mistake, however: our intent is not to replace your current IT leader or team. In fact, we rely on the expertise that your IT department has about your systems. That's what makes up the "co" in "co-managed IT."

In order for co-managed IT to work, your company's IT department will need to see us as an ally in doing their job, not as an adversary. At the same time, they'll also need to be open to new ways of doing things. The world of cyber security is constantly changing, and if your IT department is set in their ways and unwilling to budge, your company will be left with an antiquated system, chock-full of valuable data that hackers and cybercriminals can easily exploit.

Finally, however, in order for co-managed IT to work, your company still must be willing to invest in its IT department. We know that the ROI might not be as clear as it is for some other investments, but trust us, the consequences of not having up-to-date IT services if (or when) hackers steal your sensitive data could financially devastate your company - or even end it altogether.

So, with that in mind, we hope you'll consider the benefits of co-managed IT and how it can make your company safe from cyber attacks and bring you peace of mind. If you have questions or would like to know more about our IT and cybersecurity solutions, contact us today at **561-969-1616**.