



# The 3 most detrimental cyber attacks and how to stop them

Interview with Scott Plichta



**Scott Plichta**

Chief Information Security Officer at CSC

# The 3 most detrimental cyber attacks and how to stop them

## Interview with Scott Plichta

In 2016, data breaches were the biggest threat to business security worldwide, resulting in an average financial loss of \$4 million per company breached, according to Ponemon Institute's 2016 "Cost of Data Breach Study: Global Analysis." This figure represented a 29% increase in the total cost of a data breach since 2013<sup>1</sup>.

With attacks on the rise, securing your company's online assets should be front and center on any CIO's task list. As a trusted partner of more than half—including the top three—of the 100 Best Global Brands as ranked by Interbrand®, CSC® has good reason to care about its security. Our Delaware-based company serves an international clientele with our domain management, brand protection, and Internet security services. For perspective, we sat down with our very own CISO for CSC® Digital Brand Services, Scott Plichta, to hear his advice on the best ways to safeguard your digital assets.

### *Interviewer*

**Who are the major actors in cyber security threats, what are they targeting, and how?**

### *Scott*

There are three main categories. There are hackers, like the Syrian Electronic Army and Anonymous, who launch attacks around the globe for political or social motivations. There are cyber criminals who are focused on financial gain. And there are nation states whose actions generally are espionage-related. Nation states target specific organizations or industries by luring individuals to websites where malware is surreptitiously downloaded to users' computers.

The threat with hackers is that they have no defined enemy. They are making a statement. And that statement can damage a company's reputation and cause financial repercussions, depending on how long it takes the company to regain control of its compromised systems. Cyber criminals tend to focus on theft, like stealing credit card information to make fraudulent purchases. They're focused more on consumers and consumer-based businesses. Nation states are known to employ tactics such as spear phishing or watering hole attacks, pretending to be trusted people or websites in order to infect victims' computers with malware once they visit a targeted website.

“It’s really worth doing everything possible to protect against these scams. And the good news is, organizations can do a lot.”



## Interviewer

**What types of cyber attacks are affecting companies today? And how can companies protect themselves and their customers?**

## Scott

DNS spoofing and DDoS attacks are big threats to companies and their consumers. But the biggest threat right now is phishing, including spear phishing, which is a phishing attempt using a specific individual’s or company’s likeness.

Phishing schemes are designed to infiltrate organizations and steal information for political or financial gain. They’ve been around for a while. Their longevity is due in part to the fact that fabricated emails are becoming more sophisticated all the time, and more convincing to the victims they’re targeting. Spear phishing is particularly effective because consumers think the email is coming from someone they know and trust. The availability of information on social media makes the research component minimal when creating a convincing spear phish.

The phishing activity in early 2016 was the highest ever recorded by the APWG since it began monitoring in 2004<sup>2</sup>. Phishing is a double whammy for corporations because it can target staff and customers. The consequences include everything from identity theft to financial loss, data breach, and brand damage.

It’s really worth doing everything possible to protect against these scams. And the good news is, organizations can do a lot. For starters, I recommend that companies

implement single sign-on as well as two-factor authentication. CSC offers two-factor authentication through Duo Security, which we use to keep our internal systems secure. Two-factor authentication services increase your protection against phishing by helping make sure that only authorized individuals can access specific digital properties. If there’s one important takeaway from this interview, it’s that implementing two-factor authentication gives you the biggest return on investment, it’s easy, and it’s cost-effective.

Something else to consider is that your domain portfolio is a target for hackers, especially if your brand is popular or controversial. For your company’s critical domains, consider the registrar and registry lock options, because they prevent unauthorized transfers of domains to the operators of phishing sites. At CSC, we recommend that our customers use both services. There are also commercial phishing detection and takedown services that keep a constant lookout for potential attacks. You’ll want a rapid takedown service so it mitigates potential damage as much as possible. So that’s another important takeaway—registry and registrar locks are a simple solution with a huge return.

Educating your staff and customers about phishing techniques is an important step too, because these attacks work by exploiting a lack of awareness. Our employees are trained and tested on security for our customers’ safety as well as our own. Without appropriate controls, a single click on a malicious link can compromise an entire organization. The combination of good technology and awareness provides a good defense against a relentless enemy.

4 The 3 most detrimental cyber attacks and how to stop them | 2019

## Interviewer

Those are the biggest threats to companies. What are some of the others they should look out for?

### Scott

DNS spoofing, mostly used by cyber criminals, is a common threat. This kind of attack isn't directly destructive, but it routes legitimate users to fake sites, which can cause major reputational damage and lost business. To thwart DNS spoofing, make sure your DNS platform is robust enough to withstand an attack. Your first action should be to consolidate all your domain names onto a single platform so you can see your domain portfolio clearly and manage it easily and more efficiently.

We're also still seeing a sustained threat from DDoS attacks, which gridlock networks by flooding them with malicious traffic. In recent years, the typical size of DDoS attacks has exploded. CIO Insight estimates that an hour of downtime can cost a business more than \$100,000, and with the average disruption lasting more than 24 hours for some industries, these attacks quickly can become multimillion-dollar problems.

Hackers are launching most of the new attacks, the vast majority of which are aimed at Cloud, SaaS, and IT sectors, as well as financial services, media, and entertainment. Companies should consider using a DDoS protection service, which can detect an attack and effectively filter out and divert malicious traffic, allowing legitimate traffic to reach its destination.

Another important level of protection is the use of Secure

Sockets Layer (SSL) certificates, also known as Transport Layer Security (TLS). SSL/TLS certificates are an established protocol for secure communications between client and server, and are a crucial resource for websites, email, intranet sites, and IP addresses. These days, all websites should be secured using these. But even SSL/TLS protections have vulnerabilities, so companies should reassess their SSL/TLS encryption cipher suites semiannually or as a vulnerability is published. A reference I currently use is [bettercrypto.org](http://bettercrypto.org).

## Interviewer

As the chief information security officer for CSC, what advice do you have for companies when protecting their digital assets?

### Scott

Keeping digital assets secure is a combination of constant vigilance and great technology. Like Andy Grove of Intel said, "Only the paranoid survive."

Fortunately, processes and technologies are keeping pace with the threats. Brands can choose from a variety of types of protection, including extra authentication, DNS solutions, and DDoS monitoring and mitigation. Choosing the right service provider to help manage your digital assets is an important factor in your business' overall protection. A provider should be able to analyze your portfolio of digital assets—including domain, apps, social media, and more—and give you advice on the best ways to protect them while maximizing your budget. Cyber crime isn't going away, but understanding how to protect your assets from any attack will go a long way toward keeping your company and your customers safe.

# Get Secure

## Four simple and cost-effective security actions you should take today:



Implement **two-factor authentication**, an affordable extra layer of security that pays for itself. Make sure the usernames and passwords used by your employees don't access anything critical.




Add **registry lock**. Adding registry lock authentication, which requires verifying credentials with a live person, can all but eliminate the danger of unauthorized changes to Domain Name Servers.



Review **DNS solutions**. Find all your domain names and consolidate them onto a single platform. You can mitigate damage with solutions that guarantee uptime in the event of an attack by routing queries to different servers or to backup databases when server locations are flooded.



Manage **SSL/TLS certificates**. Implement SSL/TLS certificates on all your websites, consolidate the management of these certificates to make sure none expire, and then set up a continuous review of all certificates against current standards. A good provider should be able to help you with all of this, but a credible reference right now is [bettercrypto.org](http://bettercrypto.org).



“Choosing the right service provider to help manage your digital assets is an important factor in your business’s overall protection. A provider should be able to analyze your portfolio of digital assets and give you advice on the best ways to protect them.”



## Sources

<sup>1</sup><http://www.ponemon.org/news-2/71>

<sup>2</sup>[http://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2016.pdf](http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf)



[cscdigitalbrand.services](https://www.cscdigitalbrand.services)

**Copyright ©2019 Corporation Service Company. All Rights Reserved.**

*CSC is a service company and does not provide legal or financial advice. The materials here are presented for informational purposes only. Consult with your legal or financial advisor to determine how this information applies to you.*