Cofense™ Industry Brief

SAY "AH!"

A Closer Look at Phishing in the Healthcare Industry

COFENSE.COM

IT'S NO SECRET...

Healthcare is a favorite – and profitable – target for cyberattacks. If you work for a healthcare company, or if you're a patient or subscriber, you're familiar with all the data the industry gathers and threat actors crave: name, date of birth, Social Security number, mailing address, email address, and probably a credit card or two.

Where Does It Hurt?

- Over 1/3 of all data breaches occur at healthcare companies[1]
- More than 175 million records have been stolen or exposed[2]
- It costs healthcare companies an average of $408 to replace a stolen record vs. the cross-industry average of $148[3]

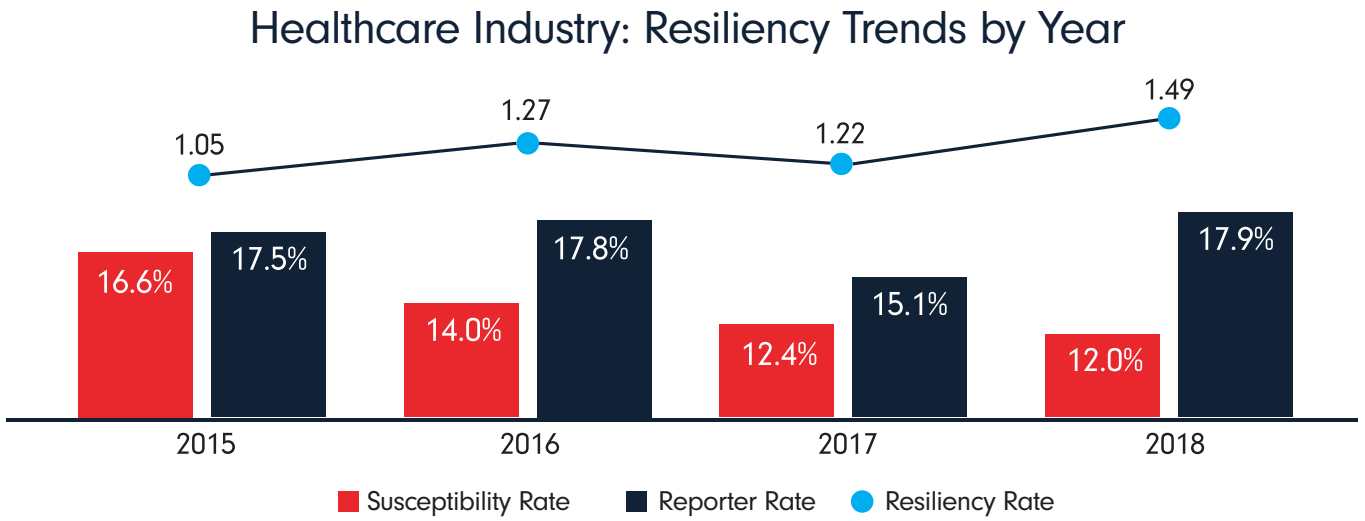
As healthcare records have steadily gone digital, the industry has played catch-up with cybersecurity. With its emphasis on patient care, in particular those aspects that drive the bottom line, healthcare has had to refocus on security and risk management. Unfortunately, in many healthcare companies, security budgets lag behind those in other industries.

That's started to change as healthcare companies pay a steep toll in data breaches: records replacement, remediation, downtime, brand reputation, fines, and even stock price. The damage happens downstream, too. When systems crash, patient care is at risk. So is the accuracy of medical records, which can result in complaints and lawsuits.

While most breaches begin as phishing emails, scant public data exists on phishing attacks in the healthcare industry. In this industry brief, Cofense™ will share data we track to clarify how phishing endangers healthcare providers. We'll also share the abridged version of a healthcare case study showing how one company stopped a phishing attack in 19 minutes.

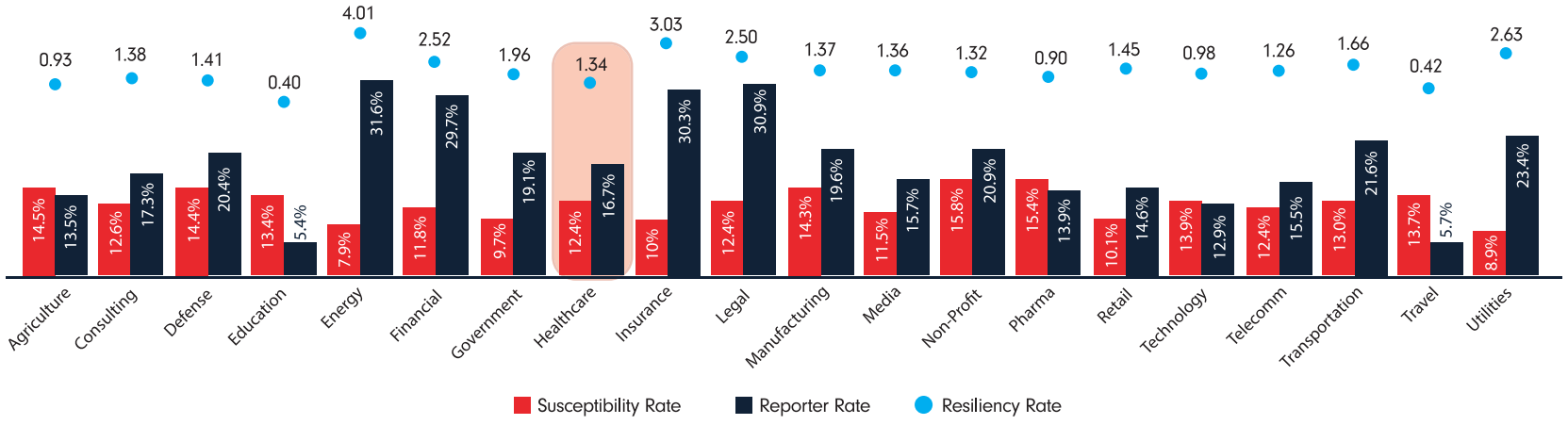
HOW RESILIENT IS HEALTHCARE TO PHISHING?

You may have heard the term "resiliency" in anti-phishing circles. Resiliency is the ratio between users who report a phish versus those who fall susceptible. In the chart below, you can see the ratio as measured during phishing simulations Cofense builds and tracks for customers. In this training, users receive simulated phishes to keep them on their toes.



Two take-aways: resiliency in healthcare has improved but not dramatically and the current rate of 1.49 is okay, though not great. Let's take a look at how healthcare stacks up against other industries.

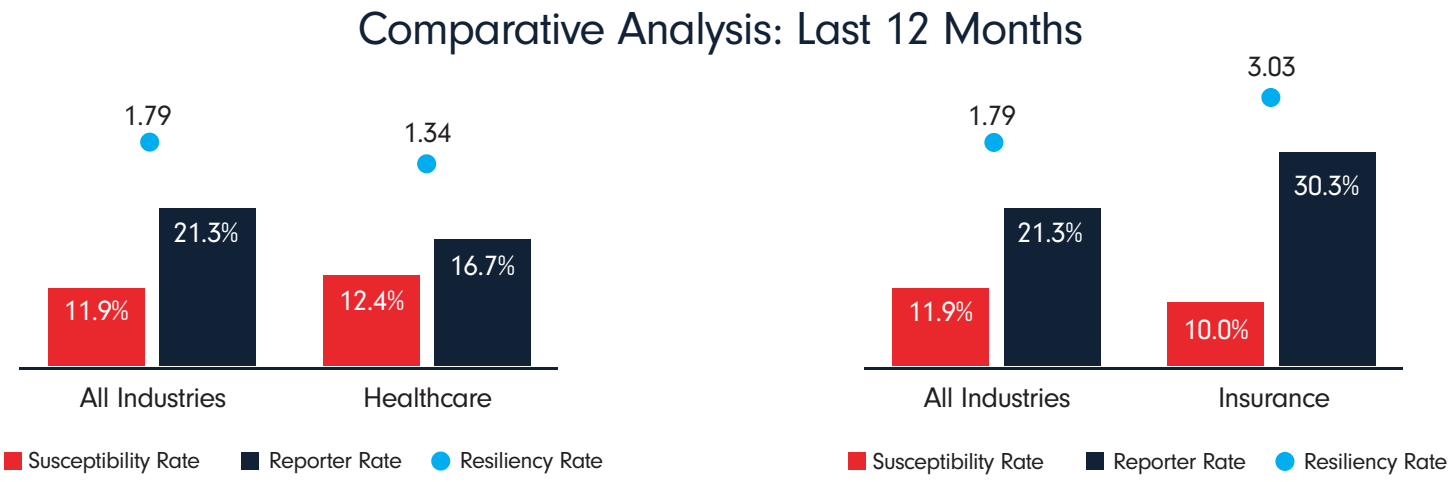
All Industries: Resiliency Analysis of the Last 12 Months



Look at the energy industry, with a resiliency rate of 4.01. Check out financial services at 2.52, plus legal services at 2.50. Clearly, while healthcare is a big target, the industry isn't leading the way in protecting itself against attacks. Yes, there are industries that fare much worse and sure, their data is valuable, but healthcare is in the crosshairs. The need to improve is urgent.

One factor that surely inhibits the industry's resiliency: high turnover. With physicians, registered nurses, and administrative staff constantly churning, it's hard to gain traction in the fight against phishing.

Here's Another Cross-Industries View:



As you can see, healthcare lags behind the aggregate resiliency rate of 20 major industries. Interestingly, the insurance industry, to which healthcare is closely tied, fares much better.

Why is resiliency higher in insurance versus healthcare? One possible reason: insurance is tied to financial services, which is frequently attacked as well as heavily regulated. According to Cofense data, the resiliency rate in financial services is 2.52.

25 HEALTHCARE PHISHING SCENARIOS

These are the scenarios most frequently used by Cofense healthcare customers. Data is ranked by percentage of users that clicked (susceptibility rate). Typically, the name of the simulation is the email subject line.

	CLICK %	REPORT %	RESILIENCY
Requested Invoice - DDE / Locky	32.5%	7.2%	0.2
Manager Evaluation (Data Entry)	28.9%	5.2%	0.2
Package Delivery	23.8%	7.8%	0.3
Halloween eCard Alert	21.5%	25.9%	1.2
Beneficiary Change	18.7%	8.0%	0.4
Holiday eCard Alerts	17.9%	2.1%	0.1
HSA Customer Service Email (Data Entry)	15.8%	12.5%	0.8
Employee Raffle	15.0%	8.8%	0.6
File from Scanner	14.7%	8.8%	0.6
Halloween Costume Guidelines	14.4%	7.9%	0.5
Unauthorized Access	14.3%	13.2%	0.9
Inbox Over the Limit	12.7%	7.5%	0.6
Order Confirmation	12.4%	11.5%	0.9
Build Your Own	11.8%	12.8%	1.1
Verify Tax Forms	10.6%	20.9%	2.0
Time Off Request - Negative Balance	9.9%	16.8%	1.7
Employee Satisfaction Survey	9.0%	5.4%	0.6
Holiday Order Confirmation	9.0%	12.7%	1.4
Password Survey (Data Entry)	8.2%	12.4%	1.5
Scanned File	8.1%	19.6%	2.4
Inactive Email Accounts (Click Only)	8.0%	12.3%	1.5
Account Security Alert	7.3%	21.8%	3.0
Log in to Download (Data Entry)	7.1%	21.2%	3.0
Password Survey (Click Only)	5.7%	23.2%	4.1
Data Compromised (Data Entry)	3.9%	17.1%	4.4

These wide-ranging scenarios show that vulnerability is spread across business and social contexts. For example, you see low scores in Requested Invoice and e-Card simulations alike. While some would argue that an e-Card would never evade their secure email gateways, remember the gaps created by BYOD. Not everyone is on the corporate network and protected by its email systems. When personal devices are exposed, a breach can easily ensue.

3 PHISHING SCENARIOS BASED ON COFENSE INTELLIGENCE

These 3 scenarios were pulled from the chart on the previous page. They are based on active threats that were found in the wild by Cofense Intelligence and quickly worked into simulation templates for our customers.

	CLICK %	REPORT %	RESILIENCY
Requested Invoice - DDE / Locky	32.5%	7.2%	0.2
HSA Customer Service Email (Data Entry)	15.8%	12.5%	0.8
Log in to Download (Data Entry)	7.1%	21.2%	3.0

While the Requested Invoice scenario aims to deliver ransomware, a plague on healthcare companies, the Customer Service and Login to Download scenarios seek to steal credentials. As you can see, resiliency to these scenarios fluctuated greatly, from a measly ratio of 0.2 to a robust 3.

Since all 3 scenarios are based on active threats facing the industry, they are especially dangerous. Any healthcare organization would be wise to prepare for them.

DON'T BE SO EMOTIONAL

Phishing attackers are masters at pulling emotional levers. Note the emotions in play throughout these 25 scenarios. "Requested Invoice" plays on urgency. "Manager Evaluation" taps into urgency too, tinged with fear, perhaps, in some cases. "Employee Raffle" is purely about the desire for reward. These are scenarios any healthcare company will want to use in conditioning employees to be careful and not take the bait.

In previous years, Cofense reported that fear, urgency, and curiosity were the top emotional motivators behind successful attacks. Now they're closer to the bottom, replaced by entertainment, social media, and reward/recognition. It shows that as Internet behavior changes, so do phishing attacks.

Of course, any active threats your company faces is fodder for training. If you manage a phishing awareness program, ask your incident responders or threat intelligence analysts which active phishing threats you ought to simulate.

3 PHISHING EMAILS HEALTHCARE COMPANIES RECEIVED

Now let's examine some real emails healthcare companies received. What are the tell-tale signs of phishing?

Dear [redacted], this is from the insurance company concerning with your health insurance. The new insurance contract is attached.
Please look over it and let us know if you have questions.
Best Wishes,
Magdalena Sanford

Email 1: Broken English

First, that's not really an email signature. Where's the sender's title and contact information? Second, "concerning with your" will get you an F in Composition 101. And referring to the healthcare insurance provider as "the insurance company" is a little vague. Red flags all around.

Email 2: Less is Less

> Hello
> Please see attached pdf file for your invoice
> Thank you for your business

An economy of words is a mark of good writing, but please. And how about some punctuation? As for "Please see attached pdf file," clicking on email attachments is never a good idea. Attacks using MS Office macros lurk in inboxes around the world. You'll want your users to examine email extensions closely—is that really a .doc, .pdf, etc.?

Email 3: Highly Targeted

> *Received Thursday, May 17, 2018 at 11:32 AM*
>
> Please find attached a copy of your 2014/15 Payment Summary (Group Certificate).
>
> **Note:** You will receive a separate payment summary for each Health Agency you worked for during the 2014/15 financial year. Payment Summaries are also available in Employee Self Service.
>
> Further information, including fact sheets: http://www.healthshare.nsw.gov.au/paymentsummaries
>
> For taxation advice information, visit www.ato.gov.au
>
> Thank you,
>
> Recruitment and Employee Transactional Services
> HealthShare NSW
>
> *This message is intended for the addressee named and may contain confidential information. If you are not the intended recipient, please delete it and notify the sender.*
>
> *Views expressed in this message are those of the individual sender are not necessarily the views of NSW Health or any of it's entities.*

This one targets healthcare employees who may have applicable taxes, a carefully defined group. The attackers did their homework. Unfortunately for them, they reference the wrong year—2014/2015 in an email sent in 2018. Like Email 2 above, this email contains an attachment.

SNAPSHOT: CRIMEWARE AMONG 3 HEALTHCARE COMPANIES

While some phishing attacks on healthcare companies come from nation-state actors, most attacks come from profit-minded criminals—no surprise, considering the healthcare industry is valued at trillions of dollars.[4] This also explains why nearly 80% of healthcare companies were successfully hit by phishing attacks in 2017.[5]

Let's examine some phishing data on 3 Cofense healthcare clients. All are national companies, all will remain anonymous. Specifically, let's look at the percentage of malicious emails among emails employees reported in the second half of 2017. Each company uses Cofense PhishMe™ to train users to recognize phishing and Cofense Reporter™ to report suspicious emails to security teams.

Percentage of Reported Emails Verified as Malicious, July-December 2017

	JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER
COMPANY 1	23.7	15.9	14.4	24.9	12.3	14.6
COMPANY 2	7.7	7.7	7.8	7.0	6.5	2.9
COMPANY 3	5.7	2.6	16.6	36.1	8.4	14.1

The Variations are Notable:

- While Company 2 had a consistently moderate level of crimeware, about 3-8%, the other companies saw significant spikes and drops.
- Company 1 swung from 23.7% to as low as 12.3%, rising again to nearly 25%.
- Company 3 started low, but later shot up to as high as 36.1%.

FYI, these shifts track with Cofense data from other industries. For example, one media company saw shifts from 14-28% while an international mining company dipped from 30% to 4% in a span of four months.

What accounts for the shifts? You'd have to ask the attackers. But perhaps what's most remarkable is the shifts themselves—the very fact that healthcare crimeware can spike to over 1 in 3 emails reported, drop the next month to less than 1 in 10, and then swing back up by almost 6 percentage points.

It's also worth remembering that a single phishing email, whether a wire fraud scam or an email delivering malware, can inflict heavy losses. Across all industries, the average cost of a data breach tops $7 million.[6] An artfully assembled and executed phish, even in a slow month, can ruin your whole year.

This underscores the need to train employees to spot phishing and report it right away. Attackers' motives and techniques constantly evolve, so healthcare companies must train users to catch the latest threats. Again, the data in the chart above stems from emails users reported. When the SOC verifies that 36% of reported emails are crimeware, the return on awareness and reporting training speaks for itself.

THIS HEALTHCARE COMPANY STOPPED A PHISHING ATTACK IN 19 MINUTES

One Cofense healthcare customer has built an end-to-end phishing defense. It features phishing awareness, reporting, incident response, and threat intelligence.

To encourage employees to report all suspicious emails, the company launched its Phishing Bounty Program. It gives cash or merchandise rewards to any user reporting a verified malicious email. Trained via Cofense PhishMe and armed with Cofense Reporter, motivated employees sounded the alarm on a well-crafted scam.

A Minute-by-Minute Recap

11:48 AM Spear phishing campaign launched.

11:49 AM Employees begin reporting the email.

11:49 AM Reported emails go to Cofense PDC for analysis.

12:00 PM As more evidence emerges, the PDC escalates its investigation.

12:07 PM Cofense completes the investigation and alerts the healthcare company.

12:07 PM The company blocks the phishing site and begins to:

- Retract the email from inboxes
- Monitor behavior coming from affected Office365 accounts
- Disrupt any lateral movement

The email very convincingly spoofed the company's CEO, asking employees to click on a link to agree to a company policy. The link went to a login page where the attackers harvested credentials, gained file system access, and attempted to reroute automatic payroll deposits.

Some employees were fooled, but many reported the email. The company uses Cofense Managed Triage™, our security orchestration, automation, and response platform. Thus, the emails went straight to the Cofense Phishing Defense Center (PDC) for both automated and human analysis.

Upon verifying the threat, the PDC notified the customer and mitigation began. Only 19 minutes elapsed from the moment employees received the email to the time the healthcare company blocked the phishing site and retracted the email.

It's common for breach detection to take over 100 days. By fusing phishing awareness and reporting with response and mitigation, this company prevented a breach in well under half an hour.

SUMMARY: PLENTY OF ROOM FOR IMPROVEMENT

The healthcare industry knows better than most that phishing is a serious problem. But the industry is still playing catch-up in phishing resiliency. Witness the 12-month resiliency rate of 1.34, compared to the cross-industries rate of 1.79.

More evidence: low resiliency to 2 of the 3 scenarios based on active threats, including rampant fake invoices, a scenario Cofense PhishMe offers and reports in granular detail. Widely embraced BYOD is a concern in phishing defense, particularly when attackers make use of social media. Cofense has helped address this problem by rolling out Cofense Mobile Reporter™, enabling users to report suspicious emails on mobile devices.

Then there are high rates of crimeware—as we've seen, in several cases nearly 25% of reported emails were malicious, while in other cases that figure reached over 35%. Again, this data comes not from simulations but active threats identified by the Cofense PDC. Real threats are getting past the industry's perimeter tech defenses. When this happens, employees trained to recognize phishing can accelerate the response by reporting emails to security teams.

To guard against the phishing onslaught, healthcare providers would be smart to create an end-to-end defense, following the lead of the company featured in the case study. A collaborative defense, built with technology and skilled humans, both users and security professionals, is the best way to lower risk.

To learn more about phishing defense in the healthcare industry, visit the Cofense Healthcare Resource Center.

Sources
1. Revisionlegal.com, 2017.
2. Hipaajournal.com, 2018.
3. Healthcare-informatics.com, 2018.
4. Infosecinstitute.com, 2017.
5. Hipaajournal.com, 2018.
6. IBM and Ponemon Institute, 2018.