Countdown to Compromise: The Timeline of a Spear-Phishing Attack on Your Organization

You are afraid. You know your business is at risk from cyber-attack. You are afraid your users are the new target and that spear-phishing is a clear and present threat. You fear a spear-phishing attack will result in a data breach that would mean you or your CEO being the next executive explaining what happened in the headlines and on CNN.

Today

"What if I'm next?" is a thought always at the back of your mind.

You can't help but think these fateful words every time you pick up a newspaper or watch the evening news. In the last year, you've seen hundreds of millions[1] of consumers and some of the biggest corporate names in the world – Target, Sony Pictures, Neiman Marcus, JPMorgan Chase, Home Depot, EMC – become victims of cybercrime.

You're afraid of being the next senior corporate officer who has to admit to missing the warning signs. You dread having to face public scorn and humiliation about your defenses being breached, the loss of sensitive information, and of admitting publicly that you were unable to protect your users and ward off sophisticated attackers.

What you're most concerned about is that attackers are using your corporate email as bait, through elaborate, highly targeted schemes. How can you think anything else, when you know that 91%[2] of all hacking begins with an email-based phishing or spear-phishing attack?

Just this morning, a colleague sent you an article[3] about spear-phishing. You read: "Hackers use spear-phishing because it works. Employees open emails and click on links. These folks are easy targets."

The article is a helpful reminder that your employees often make life easier for attackers by being the weakest link in your network defenses. Social media is a rich hunting ground for hackers. Names, locations, photos, interests, connections, partnerships, vacation details, email addresses and phone numbers – this is often the information that hackers use to target specific employees through well-crafted, highly personalized emails.

[1] http://www.newsweek.com/2014-year-cyber-attacks-295876
[2] http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/
[3] http://www.bankinfosecurity.com/spear-phishing-bigger-concern-in-2015-a-7742/op-1

With all of this on your mind when you get to work, you ask for reassurance from your IT team. They know how concerned you are about an attack, so they tell you they're ready and that your anti-virus protections are up-to-date and the firewall is patched. Did they miss an opportunity to protect your business though?

Tomorrow

You still can't get your mind off of spear-phishing. You think back to a cybersecurity conference you attended last year, and remember being startled at how many of your peers claimed they were sufficiently protected from cyberattacks, and specifically spear-phishing attempts.

When you got back from the conference, you told your CEO about the spear-phishing threat, in hopes you'd get more budget for your department to help prevent attacks. You explained that 23% of phishing emails are opened and 11% of recipients opened an attachment[6]. You told him that many employees are all too quick to click on links and download attachments without thinking. Despite your attempts to sound the alarm, the CEO wasn't convinced.

Now, a year later, you're still reading about spear-phishing. To try to put your mind at ease, you write up a company-wide email to remind employees of what to look out for when they're using email. You tell them to avoid clicking on suspicious email links and attachments, even if they appear to be coming from someone or an organization they know, and to be careful about giving out personal information online.

Hopefully, they read your email.

The Next Day, and the Next, and the Next…

It's been a week since your email went out. The threat is simple; all it takes is one duped employee, thinking that an email was coming from their fiancé, sister or coworker, and then downloading or clicking the wrong thing, to put your whole company in jeopardy. The stories of the phishing used in the Sony Pictures hack make your blood run cold.

That's why spear-phishing messages are so effective. They're designed to pinpoint and exploit human weaknesses by masquerading as safe messages from known contacts. It doesn't matter if you've drawn up what you think is the perfect blueprint to protect yourself – spear-phishing attackers have done advanced scouting of your company's defenses and know exactly how to exploit vulnerabilities, the human vulnerabilities.

Now that you think about it, maybe that company-wide email you sent wasn't enough…

So, you send your own IT staff an email. You remind them that these attacks do real damage. You ask for their diligence.

The average cyber-attack in the United States costs $12.6 million per incident, while Germany ($8.1 million), Japan ($6.9 million), France ($6.3 million), the UK ($5.9 million) and Australia ($3.9 million) trail just behind.[4]

91%
of hacking attacks begin with a phishing or spear-phishing email.

From 2014 to 2015, the average information security budget dropped by **4%**, while security spending stalled to **3.8%** of the overall IT budget.[5]

[4] "Average costs of cyber-crime in selected countries as of June 2014," Statista.
[5] "Global State of Information Security," Pricewaterhouse Coopers.
[6] "2015 Data Breach Investigations Report," Verizon.

While you're thinking you've finally done everything you can to prevent a spear-phishing attack, you know you're never really safe. And the reality is, you're right.

In fact, your company is already a target, and has been for some time.

Human error was involved in more than **95%** of all cyber security incidents investigated in 2013.[7]

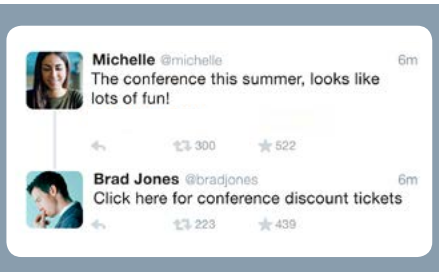
The Day of the Attack

Business continues as normal, and you are unaware that your organization is in the crosshairs. You have no idea that attackers have already sent targeted emails to Michelle in your Accounting department. Some of these emails contain malicious links, but many don't. They won't send the main attack until they've built her trust.

In November 2014, global businesses lost a combined **$594 million** due to phishing attacks.[8]

In this case, Michelle is just the weak link they hoped for. She shares so much of her personal life online, she's made it easy for attackers to learn her weaknesses. They'll use that knowedge to convince Michelle, over the course of a few months, to come to a professional conference – a conference booking that, of course, does not exist, and is merely bait to get her username, password, social security number or even bank or credit card number.

The irony you don't know yet, is the timing of the attack. Today is also when you receive a lengthy, high-priority email from your CEO. On a long flight yesterday, he read a magazine article all about the cyber threats facing businesses, and what CEOs should be doing to make sure they're protected.



He wants your immediate assurance that your company is protected and that the technology in place is doing its job.

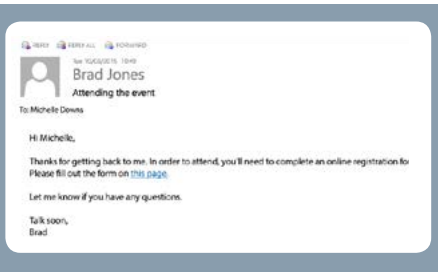
You understand why your CEO is so persistent – he, like you, is being driven by fear. Data breaches can cost CEOs their jobs. And he's putting all the pressure on you and your staff to make sure the company is protected and employees are well-trained. If only you'd known then that the attack against your company had already happened, and that your fate was already sealed…

[7] "IBM Security Services 2014 Cyber Security Intelligence Index," IBM.
[8] "Monthly Online Fraud Report – December 2014," RSA.

The Weeks After the Attack Starts

Unbeknown to you, threat actors are continuing to send emails to Michelle. Your IT team is unaware you're being targeted. Everything appears normal.

Eventually, your attackers build trust with Michelle.
Finally, the attackers send the real email bait. It's an innocent looking link in an email. Michelle, who has already fallen victim to social engineering, won't think anything of it.
She clicks the link.



She's immediately sent to what looks to be a safe website, but it's actually just a front for a malicious webpage, where Michelle will unknowingly give away her network credentials and credit card information, and allow malware to be downloaded to her desktop.

And with that, the attackers are in! The malware is downloaded and deployed across your systems, releasing sensitive information right into the waiting arms of your attackers.

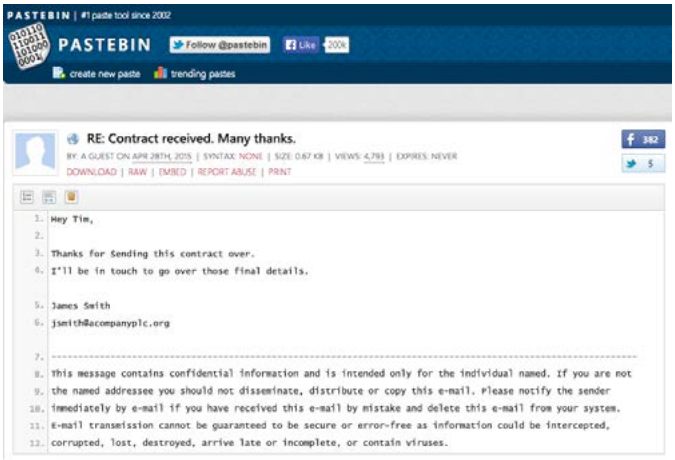
The Day of Discovery

The 3 a.m. call startles you, and you know immediately what's wrong. You knew this day would come.

It's a member of your IT team. He has detected the presence of malware on the network. Your staff is able to confirm the breach after finding traces of your data – from customers, users and suppliers – on Pastebin and across the Internet.

And while you don't know it now, your information has actually been exposed for 232 days.

You hang up and start dialing your CEO. You finally have to deliver that message, that there's been an attack and that data has been stolen.



One Day After Discovery

After an around-the-clock investigation, your IT team determines that the attackers used a spear-phishing email against Michelle.

They've shown you the email, with its clever social engineering and a link to their malware-laden website. It looks convincing – you're not surprised she fell for it, even after your email and countless other warnings. But then again, that's the idea isn't it? The reason you had all those warnings was because spear-phishing attacks exploit the human weaknesses in your organization and are difficult to foil.

The average company goes
229 days
before realizing it's been breached.[9]

[9] "2014 Threat Report: Beyond the Breach," Mandiant.

Three Days After Discovery

The clean-up continues.

You now know that your entire customer database and billing records have been stolen, and you're working with your team internally to notify those customers.

Then, the next domino falls. You get your first inquiry from a news outlet. Soon after, every major news organization – MSNBC, CNN, Fox, BBC, Sky News, the Telegraph, RT – asks for an interview with you and your CEO. Your only hope now is that you can help your CEO recover.

As the CEO talks about next steps and moving forward, that's exactly where your mind wanders as well. What more could you have done to prevent the attack? If only you'd got your team to deploy some sort of anti-spear-phishing technology, the picture could have been a whole lot different.

Sometime in the Future

You're still working out the total cost of the breach. When you add together the cost of detection, reaction, clean-up, further breach mitigation, notifying and reimbursing your customers and clients, updating your security infrastructure, PCI fines, the cost of the reputational damage – to say nothing for the ongoing lawsuits from your customers and clients – you're still losing sleep. You know these costs can climb[10] to over $200 million easily and quickly.

You're hoping that by improving employee awareness of cyberattacks and instituting new cyber defenses, particularly your new Targeted Threat Protection system, you've done enough to prevent another spear-phishing attack.

You're still fearful of another incident – that feeling will never go away – but for now, you feel your company is as well-protected as it's ever been.

With Targeted Threat Protection, CIOs, CISOs and IT department heads gain real-time protection against targeted spear-phishing attacks, the peace of mind that goes with it and a fail-safe for when employees invariable click on the wrong link or download the wrong attachment.

For more information about Targeted Threat Protection visit www.mimecast.com

"Like all of you, I've been shaken by the news of this attack," your CEO says in his first interview, "It's my promise today, to every single one of our customers that we will work tirelessly in the coming months and years to get to the bottom of this attack and prevent it from happening again. We will earn back your trust…"

Target's Data Breach Costs Now Total
$236 Million[11]

[10] "http://digitaltransactions.net/news/story/Target_s-Data-Breach-Costs-Now-Total-_236-Million

[11] "Target's Data Breach Costs Now Total $236 Million,"Digital Transactions.