# Breach Is Not Inevitable

*PhishMe's Rohyt Belani on How to Empower Employees to Bolster Defenses*

*Good news: The time to detect data breaches has gone down. Bad news: It's still 146 days on average.*

It has become accepted in many security corners that "breach is inevitable." But Rohyt Belani, CEO of PhishMe, rejects that notion. Hear how he believes organizations should be arming their employees to help fight back against attackers.

In a video interview at RSA Conference 2016, Belani discusses:

- The latest phishing schemes and why they succeed;
- Why breaches are not inevitable;
- New technology solutions that help bolster enterprise defenses.

Belani has more than 14 years of experience in the information security industry, with prior roles including cofounder and CEO of Intrepidus Group (acquired by NCC Group), managing director at Mandiant, principal consultant at Foundstone (acquired by McAfee), and researcher at the Software Engineering Institute. He has served as an adjunct professor at Carnegie Mellon University and is a contributing author for "Hack Notes - Network Security and Extrusion Detection: Security Monitoring for Internal Intrusions."

## People Can Be Leveraged

**Tom Field**: A year ago, we sat and talked. At that point, you had just introduced a new solution that aimed to prove that people were not the weak link in security we always hear about. You've had an opportunity now to get this product in the market. How has your theory of people actually being a strength played out?

**Rohyt Belani**: Fabulously well. If you think about physical law enforcement, for example, they've always used human informants very effectively. For some reason cybersecurity has continued ignoring the human thus far, thinking of them just a weak link that needs to be rectified. We turned that message around, saying, "No, you can actually leverage them," and we're finding the results are amazing. Attacks are being detected within seconds of them reaching inboxes versus relying solely on technology.

## The State of Phishing 2016

**Field**: I want to talk with you about the state of phishing in 2016 because it seems behind every great breach, there's a great phishing scheme. How do you characterize the threats that you're seeing predominantly today?

**Belani**: A lot has changed, and a lot hasn't. I've been in cybersecurity for 14 years now. At least for the last 10, phishing has been the dominant vector. The attackers may have changed a little bit. There's the flavor of the year, so to say. It's the nation-state versus ransomware, cyber criminals versus the folks behind business email compromise and CEO impersonation.

We just heard about Snapchat getting compromised. What we're finding is that there's a common thread. It's phishing that's being used. That part hasn't changed. It's the type of attackers and the motivations that are constantly changing. That's really the challenge for companies like us helping our customers to understand the nuances, to give them the technologies to best protect their people.

**Field**: If one were to look at the news, one would say that "No, organizations are not any better at detecting and responding to phishing threats." How would you counter that?

**Belani**: I wouldn't make a blanket statement that we aren't better. We've made some strides there, but it's still far behind the curve. There was a recent report by a company called Mandiant that said, "Good news: The time to detect data breaches has gone down. Bad news: It's still 146 days on average."

146 days.

**Field**: We've lost 100 days.

**Belani**: Exactly. We've come down by about 60, but we're still 146 days behind the attackers. We're lagging there, but we are moving in the right direction. That's the positive, the silver lining.

**Field**: How then are the fraudsters in turn responding to our defensive efforts? Because we've found consistently their best offense is a better offense.

**Belani**: The attackers are obviously extremely resourceful and smart. They realized a lot of the defensive controls were geared towards identifying malware, files that are attached to emails. What they said is, "Look, if that's what you're really looking at, I'm just going to a different way around this. I'm going to change the malware, maybe go malwareless," which is the CEO impersonation attack that we're seeing.

Two billion dollars have been lost to that specific attack vector in the last year by U.S. companies alone. Ransomware, as

*My VP of finance received an email where they tried to impersonate me, asking him to wire out money. The email said, "Sent from my iPhone," and he knows I use a Samsung phone. It took him all of eight seconds to identify that it was a phish.*

we all know, has picked up. A lot of these attacks are either malwareless, or they're using malware that no one has seen before. Really, the focus is on social engineering people. That's where we say, "Let's address the root cause versus the symptom here."

## Writing Humans Into the Security Posture

**Field**: Tell us about how you do that, given that technology is not going to solve a malwareless attack. What are PhishMe's opportunity and your edge?

**Belani**: Our edge is we write humans into the security posture. There was a Time Square bombing that occurred back in 2010, which was detected by two T-shirt vendors who saw a smoking Nissan Pathfinder parked smack in the middle of Times Square. They said, "Contextually, this is not what I see every day." Neither the surveillance systems in place nor the cops on Segways and horses identified this.

Leveraging the human element clearly works. To give you an example, when phishing emails come in, typically it's not about the malware or the technical characteristics of it. My VP of finance received an email where they tried to impersonate me, asking him to wire out money. The email said, "Sent from my iPhone," and he knows I use a Samsung phone. It took him all of eight seconds to identify that it was a phish, and this email went through every piece of defensive technology because, believe you me, we use them all on our mail servers.

## Simplifying the Informant Process

**Field**: As a security technology vendor, your people are aware of these challenges. How can a typical organization hope to cope?

**Belani**: People can get conditioned very well to the things we learn from all sorts of domains. Marketing people change our mind every day and get us to do things we may not want to do in the first place, like buy things. With cybersecurity, we learn we can condition people to have their radar screen on, and more importantly, show them the value of them turning into informants. Give them the tool. Take away the friction.

If you tell people, "You've got to pick up the phone, call the geek in the back room, and explain to him what happened," it's not going to happen. If you give them a tool to say, "Click this button when you see a suspicious email," all of a sudden, they're doing

it, and the IT teams are liking that too because they're getting what they need without having to go back to explain, "How do you rip out headers from Outlook?" or "It's a 10-step process that I have to walk you through." A lot of it is conditioning the employees, taking away the friction, and cutting to the chase.

## Infections Are Inevitable; Breaches Are Not

**Field**: It's become cliché in the industry to say breach is inevitable. You completely reject that?

**Belani**: Right.

**Field**: How do you counter that notion?

**Belani**: I counter that notion by saying I think individual infections are inevitable, not the breach. The breach is when they have been on your network for 146 days, post multiple infections, they've found their way to the crown jewels, and none of your detection controls have worked. We believe that while there might be minor infections, if you put the right canary in place and you have the right detective controls, you will find things before they turn into breaches.

Again, there isn't a better mechanism than humans who are contextually aware

*If you tell people, "You've got to pick up the phone, call the geek in the back room, and explain to him what happened," it's not going to happen. If you give them a tool to say, "Click this button when you see a suspicious email," all of a sudden, they're doing it.*

asking, "What is that about? Why is my computer behaving strangely? Why did I get that strange email?" It really works in cutting it short. Yeah, they've been on the system, the dwell time as we call it, to seconds and minutes versus the hundreds of days.

## Magnifying Human Intelligence

**Field**: Talk to me about new solutions that PhishMe has brought to market that help organizations to analyze both data from internal attacks as well as external.

**Belani**: We brought a couple of new products to market this last year. PhishMe's Triage Solution is a sort of a human intelligence management system. It's all the human intelligence that comes in from your conditioned employees. It actually suppresses the noise because there is a lot, and helps the incident responders manage the workflow, analyze things and most importantly, operationalize it.

How do I convert this into rules that I can push into my mail servers, into my firewalls, and so on and so forth? We're going to be making some announcements about technical partnerships and alliances. It's a who's who list of cybersecurity. Every one of these vendors now wants to partner with us.

We also acquired assets of Malcovery Security, which focuses on threat intelligence specific to phishing on the external Internet.

If the NYPD found a suspicious person with a backpack and someone called it out and if you also knew that Scotland Yard found a suspicious backpack in a Duke station, you combine the two. The power of that knowledge combined is way greater than just that one isolated incident. That's the power we're trying to bring to cybersecurity here.

## How to Avoid Becoming the Latest Ransomware Victim

**Field**: We've talked about CEO compromise and ransomware. What are the attack vectors that concern you the most for this year ahead, and how are we going to be able to respond to them most appropriately?

**Belani**: I will say what I've said for about seven years now. In 2012 I said, "This is going to be the year of the phishing. Can I go back and say how short-sighted I was there?" Every year seems to be the year of the phish. Unfortunately, this technique of social engineering has worked for hundreds of years in the physical land, and it's going to continue in cyberspace.

Cyberattacks are very lucrative for cyber criminals, as we found with ransomware, and I do think that that's going to be something that we're going to have to contend with even more. What is scary to me is as the Internet of Things picks up and people's pacemakers are connected to the Internet and whatnot, there is the potential for personal ransomware like, "Hey, I'm controlling your pacemaker. Do you want me to turn it off or pay up?" It is pretty scary.

As industrial control systems are increasingly online, people can access dams and power grids as we found when the Ukraine grid was shut down from a cyberattack. We're going to see a lot more of control system ransomware exploitative nature of attacks, much more so than we've seen in the past. It's not going to be just nation-state actors. They're going to continue existing, of course.

**Field**: What do you advise your customers when they come to you and say, "We're victims of ransomware?"

**Belani**: Yeah, it's a tough one. The FBI has actually been advising to pay up. In some cases, there is no choice but to do that, unfortunately, because the preparation leading up to these has been flawed. While of course, we can do things to reduce the risk up front, get conditioned people who don't fall for the attack in the first place or it gets detected, there are several other things that can be done.

If people have a strong backup policy of their systems – if they're backing up not incrementally, but fresh backups on a periodic basis – you can say, "Look, it's locked on by ransomware. I can just go back to yesterday's backup." Most people to save storage are doing incremental backups. Then your incremental backup is corrupted. Having a strong backup strategy followed by roping the human into it and having phishing defenses in place is really at the core for being able to prevent ransomware from succeeding.

## Privacy vs. Security

**Field**: Can I ask you a question as a security executive? As a leader in this industry, we have everybody now talking about the Apple case with the government saying, "Apple, we want you to help us get into this iPhone." How does that strike you as a security leader?

**Belani**: I don't think there's an easy answer there as well, right? Look, you have to weigh the pros and cons, and it's always security versus privacy and then you talk about people's lives at stake. Then on the other hand, you say, "Well, where does this stop then? If we give you access to this, if I have something in my mind, now is that something I'm obligated to tell you as well because it's a security concern?" I just don't know where this stops.

I would say I'm far from qualified to actually say, "This is the right way to do it." I know FBI and Apple are on Capitol Hill today testifying, and I'm watching it very closely to see where this goes. ■

## About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

## Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com