‘Inside a Data Breach’

Script	Visual Concepts
RSA. Target. Neiman Marcus. The roster of enterprises who’ve suffered a data breach -and the associated costs of recovery- grows longer every day. More than half of all small and mid-sized businesses have been hacked and three-quarters say they can’t restore all their data.	Dan’s talking to the camera/viewer in the hallway outside the entrance of ToB’s offices.
Reacting to new threats is too slow and too expensive. These days, you have to preempt by concentrating on the *methods* of attack.	Dan starts to walk down the hallway, passes the ‘target employee’s’ office in the background, and keeps going.
Fortunately, attackers are just as fallible as everyone else. They’re naturally inclined to focus on easy targets and primarily use the two methods of attack with the greatest chance of success: phishing and watering holes.	Dan stops in front of the ‘Attackers’ office’ where a small group is diligently working on their computers to compile a new attack. Several are discussing a ‘play’ on a whiteboard.
In a typical phishing attack, your employees receive socially engineered emails with a toxic attachment or link, and a convincing reason to click.	Combine a series of frames of the attacker group doing their business.
No amount of training can guarantee that all of your employees will detect phishing emails all of the time. That’s why phishing attacks are so common, and why they’ll never go away.	Show the ‘employee’ reading an email and clicking on a link. (For dramatic effect,) the employee recognizes that s/he has been duped. The screen shows a Jolly Roger.
More sophisticated attackers now use "watering holes;" malicious code installed on trusted websites.	Return to the attacker group doing their business.
For example, if they wanted to attack a Goldman Sachs, they would put malicious code on a low-security web	Show the same ‘employee’ navigating to

forum discussing quantitative trading strategies. By going to this forum, every visitor would come under the attackers' control. They could sort through the victims later.	a forum and clicking on a link in a discussion. This time, the employee doesn't recognize that s/he has been successfully attacked.
Watering holes are invisible to users. There is no training to avoid them. This approach is becoming more common.	Dan standing outside of the 'employee's' office where the audience can clearly see that the employee is unaware of the attack.
Before you know it, a compromise on one device could spread to your company's entire network, to your business's bank account, and on to your business partners.	Dan starts walking down the hallway to his office.
Does it sound like black magic? It's not. It's just business. To get set up, attackers have to invest in equipment, code, and people. They establish a system of operations -a playbook- and they work toward a return on their investment. Just like a business.	Dan passes by expensive looking equipment. (Does ToB have some sort of server rack?)
Every time one of their attacks succeeds, they leave a trail of bits. To cover their tracks, they should dispose of the equipment after each attack. But who wants to restart from scratch after every project? Why not apply that successful play to another easy target? By taking an attacker-centric approach, focusing on the most high-risk employees, and probing vulnerabilities in your email and browser, we can reverse engineer their playbook. And then we know what to watch out for. It won't stop attackers altogether, but it will deflect them away, to easier prey.	Pan over the whiteboard seen in an earlier frame. This could be a good use of that accelerated white-board animation that's so popular right now. The handwriting should be clear, but the illustration doesn't have to be anything special.
What can you do about all this today? 1. Use a dedicated computer for online banking, so sensitive information is separate from social	Dan sitting down on a fancy couch in his sweet penthouse office.

information. 2. Configure your email securely, so spoofed emails are caught before they're clicked. 3. Ensure that your browser keeps your employees safe from watering holes. 4. Educate your employees, beginning with the most visible and vulnerable. 5. Think like an attacker. Evaluate the entire chain of events in a possible attack, and address weaknesses. 6. Automate automate automate. Your defenses should always be working, and always updated to reflect the latest attack techniques.	There's another white board beside him with each of these bullet points listed in short form: *1. "Compartmentalize* *2. Secure your email* *3. Configure your browsers* *4. Prioritize vulnerable employees* *5. Think like an attacker* *6. Automate"*
For more information, go to JavelinSecurity.com	End screen is blank, aside from the logo/URL