Advisory

MARCH 2014

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

MICHAEL MCGINLEY
203.363.7368
mmcginley@wiggin.com

'Kill Chain' Analysis of Target Data Breach is a Chilling Read for Corporate Cybersecurity and Privacy Professionals

A staff report on last year's consumer data breach at Target Corporation, released today by the Senate Committee on Commerce, Science and Transportation (Rockefeller, D-WV, Chair), provides a gripping wake-up call for those who oversee the security of corporate America's systems and data. Publication of "A 'Kill Chain' Analysis of the 2013 Target Data Breach"[1] coincided with the opening of hearings by the Committee on federal legislative responses to rapidly increasing and sophisticated threats to consumer privacy and corporate cybersecurity.

STEP-BY-STEP DESCRIPTION OF THE INFILTRATION OF TARGET'S SYSTEMS AND EXFILTRATION OF TARGET'S DATA

The "Kill Chain" report provides a detailed account of the Target breach timeline based on forensic reports and other information currently publicly available, some of it unconfirmed. Russian hackers likely gained initial access to part of Target's systems using system credentials stolen from a Pennsylvania-based HVAC contractor to Target. The contractor had remote access to part of Target's network used to support electronic invoices, contract proposals and project management with outside vendors. Through the use of "phishing" e-mails sent to the HVAC contractor, the hackers appear to have obtained the contractor's passwords to the Target network.

The data thieves then leveraged their initial foothold to penetrate deeper into Target's systems, including systems that collect and store customer data. The exploit ultimately enabled the thieves to infect Target's point-of-sale (POS) systems with "BlackPOS" malware, enabling capture of unencrypted credit and debit card data as it was swiped through POS terminals at Target stores. The data was surreptitiously moved through Target's network and then exfiltrated via file transfer protocol (FTP) over the Internet to various global "drop sites." From these sites, the card data could then be sold in underground black market forums, known as "card shops."

A timeline in the report suggests that the whole process of compromising Target's systems, from the initial attack on the HVAC vendor to the theft of between 70 and 110 million customer records, took approximately two months. Just prior to the suspected initial network intrusion, Target had been certified as compliant with the Payment Card Industry Data Security Standard (PCI DSS).

WHAT MIGHT TARGET HAVE DONE TO PREVENT OR LIMIT THE CYBER ATTACK?

The Committee's report emphasizes that the full details of how the attackers managed to obtain remote "command and control" over parts of Target's systems are not yet known. Target's own forensic investigations are continuing. Nevertheless—and perhaps somewhat in speculative, Monday-morning-quarterback fashion—the report sets out a list of potential missed opportunities and "might have beens" in the collective cybersecurity practices of Target and

CONTINUED ON NEXT PAGE

'Kill Chain' Analysis of Target Data Breach is a Chilling Read for Corporate Cybersecurity and Privacy Professionals CONTINUED

its HVAC vendor which may have made the hackers' job easier. These suspected practices include:

- Target's HVAC vendor may have used anti-malware software that lacked widely-used real-time monitoring features, and one or more of its employees may have fallen victim to the hackers' phishing e-mails, allowing access to the vendor's passwords for Target's e-billing system
- Target did not use two-factor authentication for all vendors permitted access to its systems
- Target's security staff appears not to have acted on automatic malware alerts generated by Target's anti-virus software
- Target's security measures—including internal firewalls and network monitoring software—were unable to prevent the hackers from expanding their initial access to a vendor billing system into wider access that enabled them to plant the BlackPOS malware on Target's POS terminals. The hackers are thought to have exploited default account names in certain IT management system software used at Target and then used those credentials to move about undetected in Target's network
- Target appears not to have maintained a "white list" of approved FTP servers, which would have blocked data exfiltration to non-approved, Russian-based Internet servers, nor to have acted on system-generated reports that customer records were being exported to those FTP server addresses

ONE EARLY LESSON FROM THE TARGET DATA BREACH: BE CAREFUL WITH NETWORK ACCESS FOR VENDORS

The Committee report is not the final word on exactly how Target's systems were so successfully penetrated and exploited by criminal hackers. It may provide an additional spur to Congress to enact comprehensive, federal data breach legislation, a concept that the Obama Administration, the Federal Trade Commission and much of the corporate community have already embraced. And the Target incident will continue to fuel ongoing public/private discussions about acceptable private sector cybersecurity measures.[2]

More immediately, the "Kill Chain" report underscores the urgency and complexity of securing corporate information assets and consumer data in an era of increasingly aggressive and sophisticated cyber-attacks on businesses. Target was hardly a defenseless, unprepared victim; it had substantial security policies and systems in place, a sophisticated information security staff, and had recently been certified as compliant under PCI DSS, the official security framework of the payment card industry.

Further investigations and the inevitable litigation may yield a complete picture of any security break-downs at Target and whether Target fell short of any applicable standard of care or statutory duty. One lesson, however, seems clear for businesses that support network or portal access for their vendors and suppliers: even a routine service contract with an HVAC supplier can become the entry point for a massive and costly security breach. In light of the Target incident, businesses should consider:

(i) conducting thorough due diligence on any vendor who will be permitted access to any part of the company's network, including disclosure of the vendor's information security policies and practices,

(ii) negotiating adequate contractual representations, warranties and covenants by vendors to comply with the customer's information security requirements, including rights for auditing and monitoring and requiring prompt vendor communication of incidents or anomalies,

(iii) maintaining adequate access controls (such as two-factor authentication) for all vendor access to customer networks, and

(iv) securely isolating sensitive network assets from systems accessible to vendors and other third parties, and actively monitor use of vendor credentials in those network areas that are not authorized for vendor access.

While measures such as these are not broadly or explicitly mandated by law for U.S. businesses—at least not yet—they are in line with existing regulatory requirements in the financial services and healthcare industries and are frequently invoked by the Federal Trade Commission in enforcement actions under Section 5 of the FTC Act. If nothing else, businesses should not assume that "low level" or "low dollar" vendors with access to company systems can never be the source of "high dollar" harm to the company.

[1] A copy of the report is available here: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883

[2] Cybersecurity Legislation: Is Congress Ready; Federal Contractors: Meet the New Cybersecurity Standards or Lose Your Government Book