Remember When? A Decade of Information Security

DO YOU RECALL what year Melissa hit? Or SQL Slammer? Do you remember @stake or Bindview? Do you know what Bill Larson, former CEO of Network Associates is doing today? How about MafiaBoy? We've got the answers to those questions. Read on as we take you on a a trip down memory lane—information security style.

INSIDE

2 **Events That Shaped the Last 10 Years in Information Security** *by Mark Baard,* Information Security *staff*

4 **10 Worst Data Breaches** *by* Information Security *staff*

5 **SOX Appeal** *by Amy Rogers Nazarov*

6 **Doing Battle: 10 Years, 10 Attacks** *by* Information Security *staff*

6 **10 Companies/Markets That Succumbed to Market Consolidation** *by* Information Security *staff*

7 **Where Are They Now?** *by* Information Security *staff*

INFORMATION SECURITY®

GETTING THE POINT

ChoicePoint put data breaches on the front page of The Wall Street Journal, into corporate boardrooms and the consciousness of Americans.

BY MARK BAARD

ChoicePoint CISO Richard Baich's protestations in 2005 that his company was the victim of fraud, not a hack, sound almost archaic now.

"This is not an information security issue," Baich told *Information Security* shortly after ChoicePoint disclosed 163,000 customer records had been accessed. "My biggest concern is the impact this has on the industry from the standpoint that people are saying ChoicePoint was hacked. No we weren't. This type of fraud happens every day."

In fact, the incident underscored the vulnerability of sensitive data to many attack vectors, from classic computer hacks to trusted insiders to thieves like the ChoicePoint fraudsters. They posed as legitimate business customers and set up accounts to obtain the type of information that ChoicePoint typically sold third parties.

It's not that ChoicePoint was the first or the worst data breach, but it was spectacular, driving countless companies to take steps to avoid ChoicePoint's miserable—and very public—experience, which was resolved when it paid $10 million in fines and $5 million compensation to consumers after it reported the breach to California regulators and consumers. ChoicePoint executives got a good tongue-lashing before Congress for good measure. In March, it was acquired by Reed Elsevier, parent company of LexisNexis.

"The message to ChoicePoint and others should be clear: Consumers' private data must be protected from thieves," FTC Chairman Deborah Platt Majoras said in a statement. "Data security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business."

But data owners still have a long way to go to secure critical information and prevent fraud, says Gartner analyst Avivah Litan.

"[Data breaches are] still happening," Litan says. Since ChoicePoint was breached, more than 215 million personal records have been lost by entities responsible for them. TJX, Gap Inc., Monster.com and TD Ameritrade last year alone.

SB 1386

If any positive changes have taken place in the data brokerage industry, it was not due to ChoicePoint's admission of carelessness, says Litan, but rather California's SB 1386 regulation, which compels data owners to reveal breaches to victims. Any company that does business in California must

| More Milestones

7 Turning Points

ChoicePoint, Sarbanes-Oxley and the advent of crimeware had company. Here are seven more information security signposts of the last decade.

DDoS Attacks Compared to today's targeted incursions on companies, MafiaBoy's February 2000 DDoS attacks on major ecommerce sites like Yahoo, Buy.com, eBay, E*Trade, CNN and Amazon seem like high-profile Internet pranks. Yet they paved the way for a rash of extortion schemes based on DDoS attacks and shook consumer confidence in online buying. One-third of those surveyed following the attacks said they were less likely to make a purchase on the Internet, and three out of five were more concerned about their privacy than before.

Code Red, NIMDA, Slammer Truly the evil trinity of early malware, Code Red, NIMDA and SQL Slammer made Windows and network administrators shiver. Code Red struck first in July 2001, exploiting a buffer overflow vulnerability in Microsoft's IIS Web server that had been patched weeks earlier. NIMDA, meanwhile, arrived a week after the Sept. 11 terrorist attacks, leading some to speculate the worm could be a follow-up attack against an already shaken nation. NIMDA spread not only via email as Code Red did, but through open network shares or

HOT SEAT Former ChoicePoint CISO Richard Baich was at the center of the firestorm in 2005 when the data broker disclosed it had been breached and the identities of 163,000 were in peril.

notify those affected by a data breach. Prior to SB 1386 and the 38 other state data breach notification acts, few companies would be compelled to inform customers of a breach and data loss.

Litan says that while laws ensure the accuracy of personally identifiable information, not enough carry harsh punishments for companies that fail to protect consumers against fraud.

"I'm not saying that regulation is the answer to everything," Litan says, "but it will take a stick

More Milestones

infected Web sites. It also exploited a hole in IIS. Slammer may go down as the most prolific and efficient worm in history. Hitting in January 2003, Slammer spread incredibly quickly through a buffer overflow bug in SQL Servers worldwide. Within 10 minutes, 90 percent of vulnerable machines had been infected (a patch for the vulnerability had been available for six months). Slammer weighed in at less than 400 bits of code, but delivered a nasty denial of service payload, slowing down Internet backbones in countries all over the world.

9/11 The Sept. 11 terrorist attacks had an enduring impact on the economic, psychological and social fabric of the United States, but was it a turning point in information security? Not to a great degree, but it did increase awareness of security, and focus attention on contingency planning and business continuity.

Spam Spam has exploded as a security and operational problem, making up 87 percent of global email by the end of 2006, according to email security vendor Commtouch. That volume spiked precipitously late last year, fueled by the use of botnets, largely replacing the buying and selling of address lists, and new evasion techniques delivering not only unwanted junk email, but a litany of phishing attacks and spyware.

Bill Gates' First RSA Keynote Two years into Microsoft's Trustworthy Computing initiative, Bill Gates put his mouth where his money was, delivering the first of his four RSA Conference keynote

Photograph by JOHN CLEMMER (veetoo.com/sb)

approach to get (data brokers) to make changes."

Businesses and U.S. government agencies—which also keep millions of consumer files—are typically guarded about the steps they take to prevent identity theft. Consumer businesses such as Target and eBay, for example, declined to be interviewed for this article. Litan says it can be difficult to convince CISOs that they need to do more to vet their potential clients.

"Data brokers make their money saying 'yes' to their customers," she says.

REAL CORPORATE DAMAGE?

They may be saying yes to more punitive damages if the torrent of data breaches doesn't subside. In addition to TJX reporting it has spent more than $250 million in cleaning up after its breach, class-action suits have been filed against the retailer, which was hacked out of more than 45 million customer records, including credit card numbers. In September, TJX announced a settlement with those affected, offering credit monitoring to 455,000 of the 45 million whose identities are at risk, the Privacy Rights Clearinghouse reports.

The Ponemon Institute in 2007 estimated data breach cleanup costs to be $197 per lost record in a data breach. TJX, however, hasn't come near that total, leading many to wonder how much damage companies suffer. Brand name damage, as well as harm to the corporate reputation, is almost impossible to quantify, but a July 2007 *Information Security* article reported that TJX's stock price remained flat throughout the crisis. Others such as Boeing and Bank of America actually saw their stock rise over a period of time following a breach.

Adam Sills, lead underwriter for Darwin Professional Underwriters, says TJX and others may really suffer when third-party costs are passed to the retailer.

"Private liability is the big unknown but it's a critical element," he says. "This is where you can probably end up seeing serious costs." ›

Mark Baard is a freelance writer for Information Security.

Infamy

NEFARIOUS NUMBERS

BELOW ARE THE TOP 10 WORST DATA BREACHES BY THE NUMBER OF RECORDS LOST.

45.7 million
Jan. 17, 2007 • TJX Companies • Hacking

40 million
June 16, 2005 • CardSystems • Hacking

28.6 million
May 22, 2006 • U.S. Department of Veterans Affairs • Stolen laptop and computer storage device

8.5 million
July 3, 2007 • Fidelity National Information Services/ Certegy Check Services • Stolen records

3.9 million
June 6, 2005 • CitiFinancial • Lost backup tapes

2.9 million
April 10, 2007 • Georgia Department of Community Health • Missing computer disk from contractor

2.6 million
Sept. 7, 2006 • Circuit City and Chase Card Services • Five computer data tapes mistakenly discarded

1.7 million
May 30, 2006 • Texas Guaranteed Student Loan via subcontractor Hummingbird • Lost equipment

1.4 million
March 8, 2005 • DSW stores • Hacking

1.4 million
Nov. 2, 2006 • Colorado Department of Human Services via Affiliated Computer Services • Stolen desktop computer

SOURCE: The Privacy Rights Clearinghouse, as of November 2007

More Milestones

addresses. It was not so much what he said on Feb. 24, 2004, but where he said it in front of an audience weary of endless patching and malware hitting Windows systems. For the record, Gates primarily previewed security in XP Service Pack 2.

Spyware Adware vs. spyware debates abated in 2004 when it became clear spyware was a security issue and machines were infected with more than just annoying pop-ups. The market was initially slow to respond. Eventually, antivirus transitioned to integrated, comprehensive antimalware tools, featuring combinations of signature- and behavior-based detection, host-based intrusion prevention, host firewalls and more. Hackers have also built business models around spyware, with large botnets spewing Trojans or hijacking machines used in everything from DDoS attacks to money-laundering schemes.

Wireless Wi-Fi liberated us, changing the way we work, making us mobile, enabling us to connect to the Internet and corporate assets at home, on the road and roaming throughout the workplace without the restrictions of wired Ethernet connections. Like most new enabling technologies, security has been playing catch-up to functionality. Wi-Fi was particularly vulnerable with a rash of insecure rogue access points and the use of hotspots to connect to corporate assets. Even reasonable precautions often weren't enough, as WEP, the first security standard, suffered from weak encryption and static keys. WPA and WPA2 standards eventually corrected WEP's weaknesses. ›

SOX Appeal

Sarbanes-Oxley Act helped put information security on the map. BY AMY ROGERS NAZAROV

THE SARBANES-OXLEY ACT OF 2002 (SOX), enacted in the wake of the accounting fraud that made Enron, WorldCom and others synonyms for financial scandal, wrought a profound change in the way businesses secure their enterprises.

Specifically, section 404—which refers to the implementation of "controls that pertain to the preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles"—has pushed countless information security professionals at thousands of publicly traded companies to consider how to deploy security practices in the service of accurate financial data. It also gave them new clout.

"SOX was a major driver at putting IT security on the map," says Constantine Photopoulos, a partner in The SOX Group, a New York-based consulting firm.

"Business knew that IT was important, but the relationship between the controls in IT and business processes became more apparent," says Sean Ballington, systems and process assurance leader, PricewaterhouseCoopers.

MISSION: CONTROL

Consider one of those business/IT links—the requirement to archive relevant instant messages—and the steps one company is taking to demonstrate the "reasonable effort" SOX requires.

"We intend to reduce [IM] issues by using Microsoft Live Communications Server 2005 and federating with MSN, Yahoo and AOL," says Jonathan Wynn, manager of advanced technology and collaborative services at Del Monte Foods' Pittsburgh site. "We're blocking clients so traffic is going through LCS."

SOX also requires that companies assess the effectiveness of their controls, then use an outside auditor to attest to the veracity of that assessment. That role is morphing, observers say.

"After seeing what happened with Enron and Arthur Andersen, consulting firms were a little gun-shy about taking any semblance of a risk-based approach to audit," says Mike Nelson, president of SecureNet Technologies, an information security consulting shop in San Ramon, Calif. "They wanted to audit every single control to the nth degree. But, in the last year or two, the Public Company Accounting Oversight Board (PCAOB)"—the nonprofit created by the passage of SOX to oversee auditors—"has focused more on the areas of the enterprise that represent the highest risk of threat."

Subsequent SOX audits have made companies more savvy. "We have reduced our key controls by one-third, from 75 to about 50," cutting audit fees in half, says Hamid Mashouf, vice president of technology at bebe, the San Francisco-based women's clothing company, which has completed three audits. "We ratcheted back because some were not needed."

Even as SOX implementation work has waned, assessment is going strong.

"We think there are more than 6,000 non-accelerated filers out there, so the bulk of the marketplace for SOX compliance is in front of us," says Rick Dakin, president and founder of Coalfire Systems, a Louisville, Colo.-based auditor.

Ultimately, SOX set the stage for organizations to meet more federal requirements. "My FISMA business is heating up," says Nelson. "SOX is cooling down."

Amy Rogers Nazarov is a freelance writer based in Washington, D.C.

Illustration by CHRIS GASH

the toughest battle: 10 years, 10 attacks

Melissa Who was looking out for an email-borne virus in 1999? Not the millions of people who opened the Word attachment that launched Melissa, replicating the email and sending it to the first 50 entries in the victim's Outlook address book, and flooding email servers in the process.

I Love You In early May 2000, this virus suckered millions of Outlook users into spreading it to everyone in their address books. "That was the first real solid social engineering attack that succeeded," says Joel Snyder, a senior partner with Opus One.

DoS Assault These crippling attacks on e-commerce sites of Yahoo, Buy.com, E*Trade, eBay, ZDNet, CNN and Amazon in February 2000 rammed home the threat of DDoS to Internet business.

Code Red Although it didn't cripple the Internet as many feared, it certainly got our attention, infecting some 300,000 servers in its first iteration in July 2001. "This one signaled the onset of the age of the Windows worm," says Ed Skoudis, cofounder of Intelguardians.

NIMDA NIMDA spread across the Internet in minutes using several propagation vectors including open network shares. "Nimda hit a week after 9/11, when everyone was emotionally drained," says Jon Oltsik, senior information security analyst for Enterprise Strategy Group. "This emotional baggage set NIMDA apart."

Root Rot Although the Oct. 21, 2002 attack was short-lived, the fact that it incapacitated or severely slowed nine of 13 worldwide "root" DNS servers by flooding them with traffic was frightening.

SQL Slammer Hitting tens of thousands of systems in a few minutes on Jan. 25, 2003, SQL Slammer launched a DoS attack that caused noticeable slowdowns across the Internet. "This one stands out in terms of propagation speed and immediate economic damage," says Oltsik.

MyDoom A mass-mailing worm, MyDoom dropped a backdoor on victim machines in January 2004, and may have infected as many as one in 12 emails, according one source.

Download.Ject and Berbew These nasties, which surfaced in June 2004, demonstrated how client machines could be exploited by malicious or infected Web sites. Sites compromised by Download.Ject would download the Berbew Trojan to visiting PCs.

Samy Aimed to spread across MySpace in October 2005, Samy demonstrated the possibility of a cross-site scripting (XSS) worm, and presaged XSS problems to come. ›

We Hardly Knew Ye

10 companies or markets that succumbed to consolidation.

SOME COMPANIES VANISH WITHOUT A TRACE; others leave their mark on a product line long after corporate entities are gone; still others maintain an identity within a new parent company. We recall 10 of the many information security companies, in some cases groups of companies, that in large part defined their markets and have come and gone:

@stake Symantec's acquisition of @stake for its professional services and talent sent shivers through the service provider's customers. Symantec seized the SmartRisk analyzer service, whose effectiveness at finding and closing network vulnerabilities drew raves from customers.

Baltimore Technologies Remember the Year of PKI? You should, because there were several. Ireland's Baltimore was one of the big names in the often rocky PKI market, but failed to endure where competitors like Entrust, RSA and VeriSign thrived. Baltimore succumbed in 2004, bought out by beTrusted at a fraction of the valuation it enjoyed at the height of the dot-com boom.

BindView A leader in risk management, its products have been integrated into the Symantec portfolio.

Brightmail The popular email security service provider is now the backbone of Symantec's services and products.

Lost Identity Netegrity, one of a handful of Web access control vendors, was snapped up by CA, while competitor Oblix was acquired by Oracle, as those heavyweights sought to compete with RSA Security and IBM in the increasingly important Web identity management market.

Okena/Entercept These companies may have been ahead of their time, when host-based intrusion prevention systems (HIPS) were an interesting technology with very limited deployment. Now, some sort of HIPS is a required component of the new comprehensive endpoint security products, and the Okena and Entercept technologies formed the foundation for offerings from Cisco and McAfee, respectively.

Poor Service The fragile confidence in managed security service providers (MSSPs) was shaken by the abrupt failures in April 2001 of Salinas Group, which shut down without giving customers passwords to access their systems, and Pilot Network Services, which shut down without notifying customers, some of whom sent engineers to the vendor's SOC.

Provisional Market User provisioning was a market unto itself within the broadly and vaguely defined identity management market, but that changed as Waveset (Sun Microsystems), Thor Technologies (Oracle), Business Layers (Netegrity) and Access 360 (IBM) were acquired to become part of more comprehensive IDM offerings.

TruSecure/Ubizen/beTrusted Remember beTrusted, the company that bought Baltimore? Well, it bought controlling interest in managed service provider Ubizen, then merged with services provider TruSecure (after it sold *Information Security* to TechTarget) to form CyberTrust, which, in turn, was recently acquired by Verizon Business.

Web App Firewalls Get Hot The startups in this market are fast disappearing, as interest in Web application security intensifies. Teros (formerly Stratum8) sold to Citrix; Sanctum to Watchfire, which, in turn, sold AppShield to F5; KaVaDo was acquired by Protegrity and Barracuda Networks bought NetContinuum in September. ›

Where Are They NOW?

CATCHING UP WITH 10 BLASTS FROM THE PAST.

1 BILL CHESWICK

Lead member, technical staff, AT&T Research

If you hate some of the clichés that are the sole domain of information security, such as the one describing corporate networks as a "crunchy shell around a soft, chewy center," point your ire at Bill Cheswick. He coined the phrase. While you're at it, though, consider that this may be the only debit on Cheswick's ledger sheet.

His contributions to network security are innumerable. A firewall pioneer, Cheswick co-authored the seminal *Firewalls and Internet Security: Repelling the Wily Hacker* with Steve Bellovin in 1994, and it remains the bible of network security professionals. The first edition sold 100,000 copies, and a second edition was printed in 2003. He also ran a project starting in 1998 with Bell Labs colleague Hal Burch to map the Internet. That data is still used to map routing issues, DDoS attacks and traceback.

"One of the reasons I did it was to get data for the researchers, and there have been papers written analyzing the data we collected," Cheswick says. "I don't know if it's changed the world particularly. The images themselves have been a marketing breakthrough." Cheswick notes the images are prominent in some senators' offices and many corporate board rooms.

After years at Bell Labs, Cheswick joined Lumeta Corp., as its chief scientist in 2000, before returning to his roots this year at AT&T Research as a member of its technical staff.

"My legacy was training the first generation of network administrators in security," Cheswick says.

The next generation? Well, for starters, Cheswick isn't so sure the Internet is as broken as everyone seems to think, considering the industry built upon it. He concedes there are security worries, but innovation in Vista and other platforms is a solid starting point. He's also aboard with the notion that the network perimeter is toast and most computers can indeed live without a firewall.

"Perimeter security was an excuse for not securing our hosts, which we didn't know how to do, or couldn't do very well," Cheswick says. "Getting out from behind the DMZ is a paper I have in mind. We have VPNs, stronger host security, crypto, a variety of tools that make us more secure. We're learning that hiding behind a wall isn't such a safe thing."

Cheswick is also aboard with virtualization and sandboxing systems.

"There's lots of commercial and academic activity on caging software. I think we have to do this because basic programs running browsers and mail readers are giant, dangerous programs that I doubt we'll ever get in secure state," Cheswick says. "You want them in a sandbox. My goal is for grandma to click on any site and not have her computer taken over."

Hear the complete interview with Bill Cheswick at searchsecurity.com/10thanniversary.

2 PETER TIPPETT

VP, research and intelligence, Verizon Business Security Solutions

Being *Information Security*'s first publisher probably isn't prominent on Peter Tippett's resume. When you're an M.D., a pilot, started ICSA Labs, pioneered security risk management metrics and, oh yeah, created the first commercial antivirus product that eventually became Norton Antivirus, media mogul takes a backseat.

Tippett was scooped up in Verizon's acquisition of Cybertrust, where he was CTO, and now he has access to one of the world's largest Internet backbones.

"There's lots of instrumentation and smart people here, but [the merger] has turned out to be even more powerful than I expected," Tippett says. "More data, reach, customers and capabilities to do pragmatic stuff on behalf of our clients and the Internet. That's been a pleasant surprise."

3 MAFIABOY

Columnist

Crime pays? Apparently so for MafiaBoy, the teen-aged Canadian hacker turned columnist for *Le Journal de Montreal* in 2005. MafiaBoy, a script kiddie, pulled off the infamous 2000 denial-of-service attacks against Yahoo, Amazon, eBay, CNN and others. The FBI and Royal Canadian Mounted Police caught up to MafiaBoy after he shot off his mouth in an IRC chat room that he had taken down Dell.com, an attack that had not yet been publicized. He was fined and sentenced to eight months of house arrest and a year of probation. In 2005, he wrote a computer security column for the Montreal newspaper.

4 PEITER "MUDGE" ZATKO

Division scientist, BBN Technologies

Peiter Zatko, leader of the L0pht Heavy Industries hacking team that became @stake, is a scientist and technical director for BBN Technologies' national intelligence research and applications division. At BBN, his work includes

developing advanced models for network data traffic analysis for the firm's government customers.

Mudge developed several security tools, including L0phtCrack, now an industry standard Windows password auditing tool called LC5. He advised President Clinton on information security, and famously warned a Senate committee in 1998 that he could take down the Internet in 30 minutes. After leaving @stake in 2002, he was chief scientist at the now defunct insider-threat specialist Intrusic before rejoining BBN, where he had worked in the '90s.

5 JIM BIDZOS

Chairman, VeriSign

For years, Jim Bidzos was the face of RSA Security, holding titles such as president and CEO, executive VP and vice chairman. He was also the emcee of the RSA Conference before stepping aside after the 2003 event. Bidzos is an important figure in the history of cryptography, lobbying policy makers in Washington to help relax restrictions on crytpo export controls, and advancing the commercialization of encryption software. Bidzos was a founder of VeriSign, where last year he returned to the job of chairman of the board of directors, which he held from 1995-2001. He served as vice chairman of the board for the past six years.

6 PETER G. NEUMANN

Principal scientist, SRI International

Peter Neumann continues his work at SRI International's computer science lab, where he is a principal scientist focused on security, reliability, voting system integrity, crypto policy and other issues. He joined SRI in 1971 after 10 years at Bell Labs, where he was heavily involved in development of Multics, a timesharing operating system. Alongside his many SRI projects, he continues to write articles, and moderate the Association for Computing Machinery's Risks Forum.

7 CHRISTOPHER KLAUS

Founder, CEO, Kaneva

Christopher Klaus, who founded Internet Security Systems (ISS) in 1994 and masterminded its groundbreaking vulnerability scanning technology, now applies his entrepreneurial and technical skills to the world of online social networking. He is founder and CEO of Kaneva, which touts itself as a "virtual entertainment world" for the masses.

Klaus was chief security adviser at ISS before IBM bought the company for $1.3 billion in 2006. In 1999, he donated $15 million to his alma mater, the Georgia Institute of Technology. Today he serves on a number of boards, including the Georgia Film, Video and Music Advisory Commission.

8 KEVIN POULSEN

Senior editor, Wired

Kevin Poulsen's high-profile hacker exploits are in the distant past. He is a senior editor at Wired News and previously wrote news for SecurityFocus. Long before he became a journalist, his hacks included taking over the phone lines of a Los Angeles radio station to ensure he'd be the 102nd caller, netting him a Porsche and cash. Last year at *Wired*, he uncovered the prevalence of registered sex offenders, including pedophiles, on MySpace.com.

9 BILL LARSON

Parts unknown

Bill Larson, former CEO of Network Associates (now McAfee), appears to have retreated from public life. During his eight-year reign at Network Associates, he oversaw 14 acquisitions and turned the company into an antivirus leader before leaving in the aftermath of an accounting scandal in 2000. Since then, Larson served on the board of directors for several technology companies, including Proofpoint. A Proofpoint spokesperson described him now only as a private citizen.

10 ERIC CORLEY

Publisher, 2600: The Hacker Quarterly

Eric Corley, aka Emmanuel Goldstein, is the publisher of the long-standing hacker magazine *2600: The Hacker Quarterly*. Corley is a multimedia figure; he also hosts a radio show for hackers called "Off the Hook" on WBAI-FM in New York, and another current events show called "Off the Wall" on WUSB-FM on Long Island, N.Y. Corley was the lone defendant in a 2000 appeal of a ruling in favor of the Motion Picture Association of America (MPAA), which wanted to bar sites from offering code that would decrypt DVDs. 2600.com was hosting DeCSS source code that could be used to beat the Content-Scrambling System used by DVDs. Corley solely took on the MPAA and challenged the legality of the Digital Millenium Copyright Act to no avail.

2600: The Hacker Quarterly continues to publish quarterly, as it has since 1984.