NewsBriefs

Brandi Ortega

Security

■ In February, **human error led Google's malware warning system to mark all search results as bad** for roughly an hour. When searchers tried to access their links, they were routed to a warning page that led to StopBadware.org. The tidal wave of searchers routed to the site temporarily knocked it offline. StopBadware.org works with Google to define a list of criteria for identifying malware sites. While updating the list, a Google worker misplaced a "/," causing it to expand to all URLs. Google's Gmail was also affected. Google has since fixed the problem.

■ In two joint surveys conducted by the Independent Oracle Users Group (IOUG; www.ioug.org) and Oracle, **only 26 percent of survey respondents said their companies apply patch updates as soon as they're released**. Roughly 25 percent of respondents also reported being behind in applying patches for at least one patch cycle; 26 percent were two to four patch cycles behind; and 11 percent said they had yet to update any of their systems.

■ In March, security companies **Fortify and Cigital released the Building Security In Maturity Model** (BSIMM; http://bsi-mmcom). Model authors Gary McGraw (*S&P* board member and department editor), Brian Chess, and Sammy Migues chose nine companies noted for taking security seriously, including Google and Microsoft, and developed a model based on the companies' common security practices. BSIMM breaks down 110 activities into 12 practice areas, including strategy and metrics, training, code review, security testing, and compliance and policy. The model isn't a security how-to; rather, it helps companies determine where their security initiatives stand compared to those used to build the model. With BSIMM, companies currently lacking security initiatives can use it to get started in creating one.

■ In March, after almost one year on the job, **Rod Beckstrom, director of the US National Cyber Security Center, quit his post**. Beckstrom resigned after criticizing the US National Security Agency's (NSA's) "control" of US cybersecurity efforts (http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf). In his resignation letter, Beckstrom wrote that letting one agency dominate cyber policy runs against the nation's democratic fabric. "The threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization (either directly or indirectly)," he wrote.

■ A **flaw in Adobe PDF viewing is much more dangerous** than previously thought, according to security researchers. Initially, Adobe recommended that users disable JavaScript in its Acrobat Reader, but security researchers have found exploits that don't rely on JavaScript. The vulnerability involves how the Reader and the full version of Acrobat open up files and could let attackers remotely execute malicious code. Adobe is expected to release a patch mid-March. The company also released patches in February to its Flash software that affected Windows, OS X, and Linux systems. These patches fixed a vulnerability that could let attackers take over machines using malicious Shockwave Flash (SWF) files. The updates also plug clickjacking vulnerabilities that enable attacks by luring users to click on certain areas of Web pages. [*Editors' note: Please see Gary McGraw's interview on p. 8 with Jeremiah Grossman in which they discuss the clickjacking flaw in more depth.*]

■ **Apple issued security updates to its AirPort Base Station and Time Capsule products** in March. The patches fix vulnerabilities that could let attackers cause denial-of-service attacks, inject forged Point-to-Point Protocol over Ethernet packets, or watch private network traffic. The updates are available through Apple's support site.

■ A **new variant of the Conficker worm is making the rounds**. The worm's controllers have designed this version, Conficker.c, to evade industry attempts to eradicate it. Several companies have banded together to preemptively register Internet addresses that the worm's controllers use to control infected machines. The new variant spews out roughly 50,000 possible URLs its owners might use, making efforts to register the addresses more difficult. The original version of the worm generated roughly 250 possible domains.

Policy

■ The state of **Massachusetts is revising its data-privacy regulation** that went into effect on 1 January. The changes to the Standards for the Protection of Personal Information of Residents of the Commonwealth will go into effect 1

May 2009. The Office of Consumer Affairs and Business Regulation is currently reviewing comments on the law but hasn't released the changes it might make. The law sets forth guidelines and processes for handling and storing state residents' personally identifiable data. The law also includes security requirements for computer systems, including mandated authentication, access control, and encryption of records and data. It requires that all data and records be encrypted when possible.

■ A **provision in the US stimulus bill that would have required employers who receive federal money to verify their workers' employment status through E-Verify has been stripped** from the bill's final version. The US Department of Homeland Security (DHS) and the Social Security Administration (SSA) run the E-Verify system, which compares information from employment applications with data from DHS and SSA databases and determines applicants' eligibility to work in the US. The free E-Verify system is Internet-based and voluntary except for federal contractors and subcontractors, who will be required to begin using the system on 21 May 2009.

■ The **US Department of Energy (DOE) is adjusting its approach to cybersecurity** after a report by experts recommended that the department use a long-term strategy that applies science and mathematics research to security. The panel of experts included security researchers from the DOE, the private sector, other agencies, and academia. Three areas of focus are mathematics to examine system behavior and anticipate attacks, information systems that self-protect and self-heal, and trustworthy platforms.

■ In March, a California assemblyman submitted **a bill that would require online mapping tools, such as Google Maps, to blur images of schools, religious buildings, government offices, and medical facilities**. Assemblyman Joel Anderson (R-El Cajon) submitted the bill in response to the Mumbai terrorist attacks last year. According to Anderson, the bill wouldn't require online mapping tools to black out these locations or stop users from getting directions to them. Rather, it would limit the level of detail available on the maps.

Privacy

■ In February, consumer rights groups raised **questions about a California Department of Motor Vehicles (DMV) plan to establish fingerprint and facial-recognition systems for issuing driver's licenses**. The American Civil Liberties Union, the Consumer Federation of California, the World Privacy Forum, and the Electronic Frontier Foundation say the DMV's plans came to light in an application for a new vendor contract to produce driver's licenses and ID cards. The proposed system would require new license or ID applicants to submit a thumbprint at local DMV offices to verify their identities. Additionally, the DMV would use image verification to match current photos with all other databases to verify individuals. The consumer advocacy groups say the DMV's plan is an attempt to circumvent opposition to biometric systems: state legislators rejected bills in 2001 to establish similar requirements. The state Joint Legislative Budget Committee has rejected the proposal, squashing the DMV's attempt to fast-track the application, but it plans to move the request forward and hold public hearings on it later in the year.

■ Several **social networking sites**, including Facebook and MySpace, **agreed to a European Union pact to guard against cyberbullying and online abuse**. By agreeing to the pact, social networking sites will provide a "report abuse" button for users. Seventeen social networks have joined in the pact. Under the agreement, social networks must set underage users' privacy settings to the highest level by default and make profiles unsearchable in search engines. The pact is voluntary.

■ In February, **Symantec introduced a cloud-based online monitoring tool for parents**. Norton Online Family can analyze a child's online presence across social networks and send out emails to parents if he or she breaks pre-established rules, such as posting highly personal content or misrepresenting age. The tool lets parents set computer-usage limits and track personal information sent via email, instant message, or social networking sites. Children surfing the Internet can send real-time messages to their parents if they come across a blocked site, letting the parents decide to allow access or not.

■ In March, **the official White House Web site (www.whitehouse.gov) switched to a generic flash video player for YouTube videos embedded on it**. Although the White House denies that the switch was due to privacy concerns, privacy advocates applaud the move. The site previously used persistent cookies in YouTube videos of the president's weekly addresses. Those who wanted to view the videos without cookies placed in their browsers had to download the videos. The new player was developed by the in-house White House Web team.

■ In March, **Google released its privacy policy for its Latitude program**, which lets mobile phone users broadcast their locations to friends. It will require warrants before sharing data with law enforcement agencies. The company worked with the Electronic Frontier Foundation to develop its position, as did Loopt, a similar service that will also require warrants before turning over users' data. □