

Hardening the Security Stack

By Steve DelBianco and Braden Cox

October 2008

The NetChoice Coalition

NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org.

NetChoice

▶ **Convenience**

▶ **Choice**

▶ **Commerce**

Protecting The Internet Against Cyber-Criminals and Cyber-Terrorists

IT security threats are becoming less pervasive but more potent. Attacks were once the domain of technically talented hackers who took intrinsic pride in taking down corporate networks and crashing consumers' PCs. Today, criminals exploit IT vulnerabilities for financial gain and hackers can disable websites of their political enemies. Perpetrators of cyber-attacks include individuals, hacker groups, terrorist networks, organized criminal groups, and even national governments.

Today's attacks can cause serious damage, as seen in the growing black-market trade in personal data used for identity theft, and politically-motivated attacks that have taken down government and banking systems. Cyber-criminals and cyber-spies are successfully evading the countermeasures deployed by most companies and government agencies over the last decade. Cyber-security should be approached as a set of complementary countermeasures at multiple layers in the security stack.

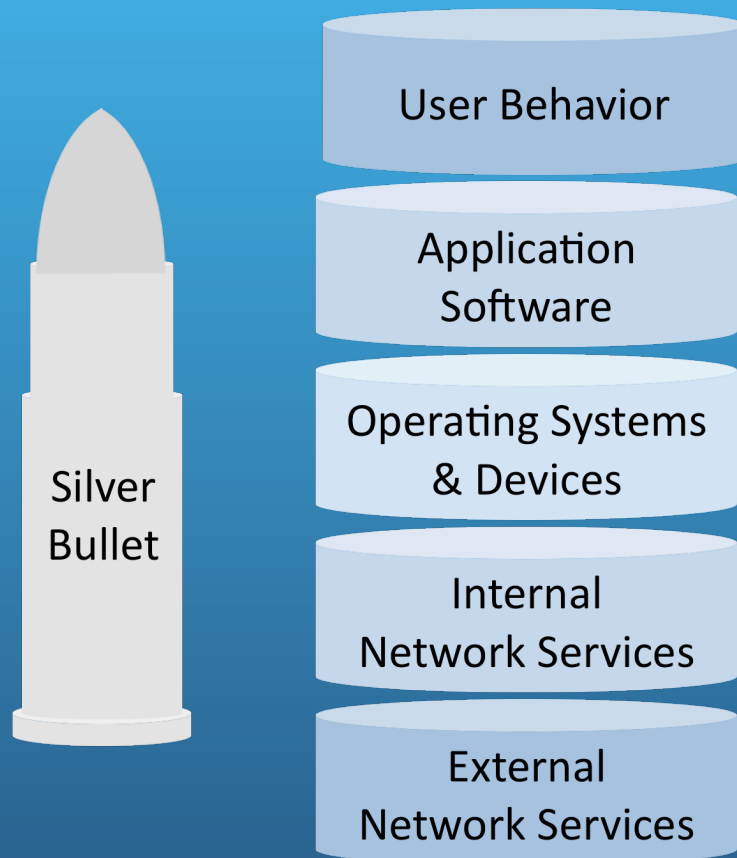


Fig 1: IT Security is a Multi-Layered Stack...There is no “Silver Bullet”

There is No “Silver Bullet” Solution for Internet Security

When confronting a complex problem or menacing threat, it's natural to search for a 'silver bullet' to slay the beast. But it's no surprise that we've yet to find the silver bullet solution for securing cyberspace. Antivirus software is necessary, but not sufficient, to fully protect computers from viruses or worms. An Internet firewall is essential for network protection, but not enough to secure an enterprise IT infrastructure. At the same time, blaming network infrastructure providers for all security problems

neglects the overall complexity of cyber-security.

Cyber-security is best understood as a multi-layered stack where threats exist at multiple levels, rather than at a single point of failure. Today's computing and networking relies on highly interconnected systems of client and server-side software, plus PC and networking hardware - all managed by corporate, government, and personal users.

There are five primary layers that comprise the security stack. (1) End-user behavior interacts with (2) application software that is installed on (3) operating systems and devices that all use network services that are (4) internal and (5) external to an organization.



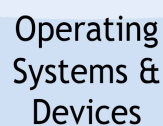
User Behavior

User behavior includes a range of security practices, from the everyday behavior of the home user to the formal security practices of a corporate user. This layer encompasses the acquisition, installation, and application of updates to security software and network hardware. It also includes user behavior regarding downloads, attachments, and links on external pages. Both enterprise and home users are fundamental to the security stack, since most attacks rely on human habits to penetrate or infect a system.



Application Software

Application software includes office and productivity packages such as e-mail, word processors, spreadsheets, instant messaging, browsers, firewall software, and anti-virus software. It also includes harmful and dangerous applications that users do not want on their machines, such as key loggers, botnet programs, and applications that siphon personal information like credit card and social security numbers. This is the layer of “zombie” applications, which turn ordinary home computers into a network of interconnected machines that are used to steal information and overthrow governments.



Operating Systems & Devices

Operating systems and devices. Operating systems, both on client and server computers, are the central layer of the security stack. On the client-side desktop environment, this layer includes Windows, Linux, and Apple OS X. Mobile devices have their own operating systems, such as the iPhone OS X, Google’s Android, Windows Mobile, Symbian, and others. Operating systems on the server-side include Microsoft Server 2008, Sun Solaris, Unix, and Enterprise Linux. While changes in desktop operating systems such as Vista and OS X have made the OS layer tougher to crack, the explosion of mobile devices worldwide is creating a target-rich environment for criminals.



Internal Network Services

Internal network services involve servers, routers, switches, VPNs and firewalls. While these devices are also part of the “operating system” layer, most of the products at this level are hardware-based, such as the Barracuda Spam Firewall, which monitors incoming and outgoing network traffic. This layer also includes routers offered by Cisco, Linksys, Netgear, SMC, and others that block suspicious traffic before it penetrates the networks. This layer is the new battleground for bot-enabled DDoS attacks, cache poisoning attacks, and network traffic ‘sniffing’ on wireless access points.



External Network Services

External network services involve the security stack layer external to the enterprise. This layer describes security functions such as packet monitoring and filtering by ISPs and Web infrastructure providers such as VeriSign. ISPs also provide spam filtering and scan email for viruses. As the Web’s traffic cops, network transport & services players are best positioned to monitor Web traffic and identify anomalies in the volume or nature of traffic such as a DDoS attack. Network transport & services players can react to these attacks by notifying or blocking affected hosts and users.

There is No “Silver Bullet” Solution for Internet Security

Every day, billions of digital communications pass through every layer of the security stack, creating multiple points of vulnerability to criminals. Moreover, the nature of cyber-security threats is changing as users put more of their life’s information online. Cyber-criminals seek to steal sensitive data, not just take down a corporate website or network.

Figure 2 shows the trail of an email as it moves through the security stack, including typical security tools deployed at each layer.

The SANS (SysAdmin, Audit, Network, Security) Institute regularly reports the top security threats, and its Top Ten Cyber Security Menaces for 2008 confirms that there has been a recent surge of increasingly sophisticated attacks, including spyware infections and keystroke loggers, that exploit browser vulnerabilities.¹ Webroot, the largest spyware

detection and monitoring firm, reports that there has been a 183 percent increase in websites that harbor spyware, and that infection rates for spyware and trojans that steal keystrokes are currently at 31 percent and rapidly growing.²

Technological hacks can be even more successful when they exploit user behavior and habits.³ For instance, criminals insert exploit code on popular, trusted websites where users have an expectation of effective security. As SANS points out, “placing better attack tools on trusted sites is giving attackers a huge advantage over the unwary public.”⁴ By attacking or spoofing websites trusted by consumers, criminals take advantage of social engineering ploys to trick people into revealing their personal information.

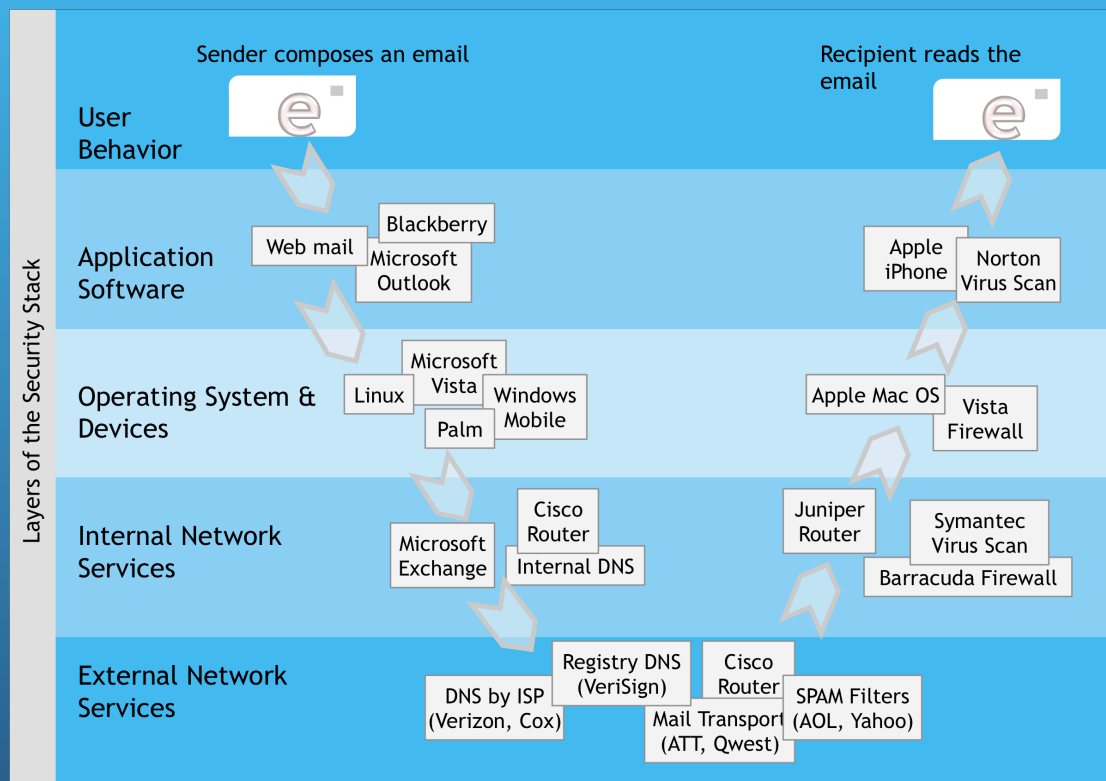


Fig 2: Trail of an Email Through the Security Stack

Social Engineering

Phishing is a type of security attack that relies on social engineering. Criminals attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by pretending to be a trustworthy entity in an electronic communication. And they're exceedingly clever in how they leverage actual events to make their phishing lures more credible.

The above is a hypothetical phishing attack, but it is uncomfortably realistic and familiar. During the October 2008 banking crisis, the Federal Trade Commission felt compelled to issue this warning: "Scammers are taking advantage of upheavals in the financial marketplace to confuse consumers into parting with valuable personal information."⁵

Technology can help reduce, but not eliminate, social engineering threats. That is why for many issues, educating users on safe practices is the key to increased security. But online businesses also continue to implement technology solutions, including toolbars, phishing filters and automated safety tests on web sites that assist users in identifying bad sites. The following tools are examples of how technology can help reduce social engineering scams:

- Some online banking sites have added measures to inhibit fraudulent access and alert users to phishing scams. For instance, the Congressional Federal Credit Union and Bank of America will challenge online users to answer out-of-wallet questions if they attempt to login from a computer they haven't used before. These two sites also display a personally-selected image to help users detect a website pretending to be their bank.
- Microsoft's phishing filter scans web addresses and pages for online Web fraud or phishing scams, and warns the user if visited sites are suspicious. It also blocks users from confirmed scams and allows users to report suspicious sites or scams.⁶ However, in the example above, this type of phishing filter would warn users from accessing wachovia.bankmerger.com only after that site was added to the blacklist.

A Hypothetical Phishing Attack

A criminal creates a website called wachovia.bankmerger.com, then sends a phishing email to a list of addresses in cities where Wachovia operates.

The email looks legitimate and logical, explaining that Wachovia's acquisition by Wells-Fargo requires users to do their online banking at a new web address. After all, users are aware of the financial crisis, and the email address and new link seem to belong to Wachovia.



When they click on wachovia.bankmerger.com, users see what appears to be a legitimate online banking website, and they enter their ID and password. By that point, a criminal knows enough to steal funds by making online payments and transfers to his own accounts.

- Yahoo's toolbar application for web browsers includes a feature called Anti-Spy, a spyware killer that scans users' hard drives for dangerous files and suspicious items.⁷
- eBay provides a tool that enables its users to protect their eBay or PayPal accounts by warning of potentially fraudulent web sites and emails.⁸
- McAfee's "Site Advisor" plug-in for Mozilla Firefox warns users before they interact with a dangerous website, and complements and enhances their existing security software by detecting spyware attacks, online scams, and sites used by spammers.⁹

DNS: Vital to the Internet - and Vulnerable to Attack

A particularly troubling security vulnerability occurs in the internal and external network services layers, where domain names are resolved through the Domain Name System, or DNS. DNS enables computers to translate host names to IP addresses, which is necessary every time users enter a domain name, click on a link, or send an email. Most DNS resolutions are done instantly by relying on a saved list of recently requested addresses, known as a cache. DNS cache tables are maintained on user computers, name servers on internal networks, and externally at the user's Internet Service Provider (ISP). If a user or application requests a URL that is not in the cache (or beyond its use-by date), the DNS performs a multi-step lookup to get the IP address from the authoritative registry for that top-level domain.

While DNS cache greatly improves performance for any operation that uses Internet addresses, it also creates an opportunity for fraud. Caches can be "poisoned" by bad actors intent on diverting users to incorrect addresses, like a web page designed to mimic your online banking site. Cache poisoning enables criminals to collect user IDs and passwords for raiding bank accounts, orchestrating identity theft, or perpetrating other forms of fraud.

In August of 2008, security researcher Dan Kaminsky discovered a troubling vulnerability in some DNS software. An attacker could flood a DNS server with multiple, slightly varied requests for a domain, hoping to eventually match a key identifier. Once the attacker has discovered this key, he can poison a name server's DNS cache, directing users to a site of the attacker's choosing.

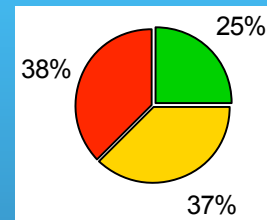
The vulnerability discovered by Kaminsky can be exploited through multiple vectors of attack. Web browsers can be forced to look up what the attacker wants, as links, images, and ads can cause a DNS look-up. Mail servers will look up what an attacker wants when performing functions such as a spam check, or when trying to deliver a bounce, newsletter, or bona fide e-mail response.¹⁰

The attention generated by Kaminsky's discovery has spiked interest in a well-known antidote to cache poisoning: a form of 'signature guarantee' for DNS lookups, through a protocol called DNSSEC. Partly in response to the Kaminsky vulnerability, the U.S. Commerce Department issued an October 2008

request for public comment on implementing DNSSEC for the "root" zone, which contains IP addresses for roughly 270 top-level domains like .gov, .com, and .org.

But DNSSEC would have to be implemented far beyond the root zone to be able to stop a Kaminsky-like attack on DNS. Afilias, the registry service provider for .org, has been testing DNSSEC on the .org domain and plans to implement it soon. And last month, VeriSign committed to implementing DNSSEC for the .com and .net domains it operates.

Kaminsky's revelation has turned out to be a much-needed boost for DNSSEC, given that early implementations have revealed thorny problems with network equipment and user applications. Most equipment in the network services is not designed to specifically recognize DNSSEC responses. This is particularly true for equipment in the internal network services layer at enterprises of all sizes. In September 2008, Nominet reported results of its test of 24 router and firewall devices used by small office/home office broadband customers.¹¹



- Just 6 units (25%) operate with full DNSSEC compatibility "out of the box."
- 9 units (37%) can be reconfigured to bypass DNS proxy incompatibilities.
- Unfortunately, the rest (38%) lack reconfigurable DHCP DNS parameters, making it harder for LAN clients to bypass their interference with DNSSEC use.

"Test Report: DNSSEC Impact on Broadband Routers and Firewalls", September 2008

Nominet's test results will give pause to anyone considering implementation of DNSSEC since they reveal that most network gear in use today won't work so well with DNSSEC. Over time, this equipment will be replaced by DNSSEC-capable devices, which could take 2-3 years at the usual rate of replacement and upgrade.

DNSSEC creates implementation challenges that go beyond network equipment, particularly in the application layer of the security stack. Operating systems include a function called 'stub resolver' that passes resolution results from the Internet to applications such as browsers. When a DNSSEC validation fails, the stub resolver passes along an error code that many browsers and applications will treat the same as a website server failure. Users won't understand these 'hard' failures when their browser fails to bring up a web page or when an email is returned - just because DNSSEC hasn't yet been fully implemented throughout a zone or website.

At the level of user behavior, the confusing errors caused by DNSSEC will likely be addressed as implementation progresses up and down the DNS. Once it is fully implemented, DNSSEC will be invisible to end users, so users will still need to maintain vigilance against phishing and fraud threats. Even though DNSSEC prevents cache poisoning, it cannot detect legitimate websites that are held by illegitimate actors.

None of the above diminishes the importance of DNSSEC as a way to improve security in the network layers. Rather, the essential point is that DNSSEC is no silver bullet when it comes to stopping cyber-security threats at multiple layers of the stack.

The next section discusses the international dimensions of cyber-security, where political tensions can motivate cyber attacks.

Cyber-Security Knows No Borders

In a world that is inter-connected by a distributed network, cyber-security threats know no political or geographic bounds. Government and corporate users need to be aware of cyber attacks from overseas.

A prominent security story last year highlighted the importance of security for governments. Congress heard testimony from senior Department of Defense officials about how federal agencies and defense contractors had terabytes of data stolen by hackers located in China and other nation states.¹²

Cyber attacks can involve disruption in addition to data breaches. In April 2007, pro-Russian nationalists initiated a distributed denial of service (DDoS) attack (in which a target site is bombarded with so many bogus requests for information that it crashes) against Estonia. This attack came in response to Estonia's removal of a Soviet war monument from the country's capital, Tallinn. The attack used botnets to deny users access to key institutions including banks, the networks of the Estonian President and Parliament, virtually all government ministries, political parties, news organizations, Internet providers, mobile phone networks and Estonian cyber response services.

Cyber attacks can also occur in conjunction with military conflicts. In August 2008, in the wake of the Russian-Georgian conflict over the Georgian breakaway region of South Ossetia, there was a coordinated Russian cyber attack against Georgia's Internet infrastructure. The attacks managed to compromise several government web sites. Georgia's Ministry of Foreign Affairs, desperately trying to disseminate real-time information about the conflict, had to resort to moving to a Blogspot account.¹³

An increasingly connected global economy inherently raises risks at multiple levels of the security stack. In 2008, the World Bank discovered a keystroke logging application running on its computers, allegedly installed by one of its IT contractors working from India.¹⁴ The World Bank also reported that its servers were penetrated by intrusions originating from a cluster of IP addresses in China.¹⁵

Cyber-Crime is Everywhere: What Can We Do?

Given the variety and range of attacks on our global cyber infrastructure, it is obvious that a single solution will not work. At each layer, vendors must provide multi-faceted solutions including better user education, hardened software applications, equipment upgrades that support new technology and vigilant infrastructure providers with the capacity to handle unforeseen attacks.

Beyond the work of each individual vendor and service provider, the government also has a role to play. Institutions such as DHS and DoD can provide unique opportunities to test new technology in a controlled environment. Government agencies that work with financial institutions should ensure that proper authentication safeguards are in place. Law enforcement agencies need to devote sufficient resources for rigorous enforcement of existing anti-fraud laws.

Where web service providers handle personally-

identifiable information, the FTC should hold companies accountable to the privacy promises they made to users. That includes ensuring transparency and accountability as to how businesses retain and share information among multiple applications and advertising partners. Moreover, when a business collects payment information such as credit card numbers, government regulators can advocate higher standards of data security.

Finally, government agencies with oversight of key Internet infrastructure should hold contract partners to a high standard on security and stability. For industry's part, CIOs, network administrators, and individual users must also evolve their approach to cyber-security. Users must remain vigilant for threats that just can't be stopped by technology.

Responsibility for cyber-security lives at all layers of the security stack, not in any one layer. Simply put, there is no silver bullet.

End Notes

¹ SANS Institute, *Top Ten Cyber Security Menaces for 2008*, available at http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10_Cyber_Security_Menaces_-_2008&ref=22218.

² SANS Institute, *SANS Top 20 Internet Security Risks of 2007 Point to Two Major Transformations in Attacker Targets*, available at http://www.sansrg/top20/2007/press_release.php.

³ Ibid.

⁴ Ibid.

⁵ Federal Trade Commission, *Consumers Warned to Avoid Fake Emails Tied to Bank Mergers*, October 9, 2008, available at <http://www.ftc.gov/opa/2008/10/bankphishing.shtm>.

⁶ Microsoft, *Phishing Filter: Help protect yourself from online scams*, available at <http://www.microsoft.com/protect/products/yourself/phishingfilter.m.spx>.

⁷ Ben Patterson, "Yahoo Toolbar," *CNet Australia*, December 3, 2004, available at <http://www.cnet.com.au/software/internet/0,239029524,240002721,00.htm>.

⁸ eBay, *Trust and Safety*, available at <http://pages.ebay.com/aboutebay/trustandsafety.html>.

⁹ Softpedia, *McAfee Site Advisor for Mozilla Firefox 26.5*,

available at <http://www.softpedia.com/get/Internet/Internet-Applications-Addons/Mozilla-Extensions/McAfee-SiteAdvisor-for-Mozilla-Firefox.shtml>.

¹⁰ Tom Espiner, "Kaminsky details DNS flaw," *ZDNet.com.au*, August 8, 2008, available at http://www.zdnet.com.au/news/security/soa/Kaminsky-details-DNS-flaw/0,130061744,339291151,00.htm?feed=pt_dan_kaminsky.

¹¹ Ray Bellis and Lisa Phifer, *Test Report: DNSSEC Impact on Broadband Routers and Firewalls*, September 2008, available at <http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf>.

¹² SANS Institute, *Top Ten Cyber Security Menaces for 2008*, available at http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10_Cyber_Security_Menaces_-_2008&ref=22218.

¹³ Dancho Danchev, "Coordinated Russia vs Georgia Cyber Attack in Progress," *ZDNet.com*, August 11, 2008, available at <http://blogs.zdnet.com/security/?p=1670>.

¹⁴ Richard Behar, "World Bank Under Cyber Siege in Unprecedented Crisis," *FoxNews.com*, October 10, 2008, available at <http://www.foxnews.com/story/0,2933,435681,00.html>.

¹⁵ Ibid.

About NetChoice

NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. NetChoice members include AOL, the Association for Competitive Technology, eBay, the Electronic Retailing Association, IAC, News Corporation, Oracle, Overstock.com, VeriSign, and Yahoo!. More information about NetChoice can be found at www.netchoice.org and at blog.netchoice.org

About the Authors

As the executive director of NetChoice, **Steve DelBianco** is a well-known expert on Internet governance, online consumer protection, and Internet taxation. Steve also serves as Vice President of Public Policy at the Association for Competitive Technology. Steve has provided expert testimony in six Congressional hearings, is a frequent witness in state legislatures, and a business leader at Internet governance meetings around the world. Steve is often quoted on technology issues in the media, including a segment on “60 Minutes” to expose barriers to e-commerce in residential real estate brokerage.

Before joining NetChoice, Steve was founder and president of Financial Dynamics, an information technology consulting firm delivering on financial and marketing solutions. He guided the firm through the rapid evolution of industry trends and sold the business to a national firm in 1997. Steve holds Engineering and Economics degrees from the University of Pennsylvania, and an MBA from the Wharton School.

Braden Cox is Policy Counsel for NetChoice and for the Association for Competitive Technology. Braden works closely with member companies to develop advocacy strategies for a number of tech-related issues, including Internet safety, behavioral ads, online marketplace liability, taxes, IP licensing and Internet governance. Braden has testified before a dozen state legislatures and regularly speaks at conferences.

Braden formerly was an attorney at a think tank in Washington, DC, where he advocated for new approaches toward government regulation of telecommunications and e-commerce. He was also in-house counsel for a startup software company. Before law school, he was a network administrator at IBM providing technical support for business and university local area networks. Braden earned his Finance degree and J.D. from the University of Georgia, and is licensed to practice law in Georgia, Virginia, and the District of Columbia.

The authors wish to acknowledge Nora von Ingersleben for her assistance in research and editing.