



ATTACK PLAN

*What are you doing to protect yourself
and your clients from cybercriminals?*

BY **PETER S. VOGEL**

COPYRIGHT ©2014

ALL LAWYERS ARE AT RISK OF CYBER-ATTACKS, AS ARE THEIR CLIENTS,

because every lawyer and client uses a computer, cellphone, or tablet to send and receive emails and text messages, search the Internet, and participate in social media. It is imperative that lawyers understand the technology they rely on. While this does not require everyone to have a degree in computer science, lawyers have a duty to protect themselves and advise clients.

According to the cybersecurity company McAfee Labs, “Cybercriminal gangs of the 21st century will target cloud-based applications and data repositories because that’s where the data is.”¹ Clearly we know that Internet cyberattacks pose a potential risk to lawyers and client files stored on computers, the cloud, or in their offices.

HOW SAFE DO YOU FEEL ABOUT PUBLIC WI-FI?

Do you use public Wi-Fi? I assume most everyone reading this article does. Based on a recent white paper from Symantec,² however, most people do not use private encryption tools despite the finding that most Wi-Fi networks are not as they seem. According to the report:

Unless the local and server applications have implemented some sort of private encryption protocol, which is atypical, ... all traffic [on public Wi-Fi networks (and many private ones as well)] is in plain text on the local network and anyone on that same network can read it.

Symantec recommends using encryption security measures including the Secure Sockets Layer,³ but most lawyers generally do not know they are vulnerable, let alone what Secure Sockets Layer is. Without question, it is time that lawyers got to know more about the technology that they and their clients rely on since there are risks associated with the many different types of devices, Internet connections, and technology conveniences.

ABA CYBERSECURITY HANDBOOK

In 2013, the American Bar Association published a *Cybersecurity Handbook* written by a number of lawyers.⁴ In the forward, former ABA President Laurel Bellows explained why the handbook was published:

The American Bar Association recognizes that cybersecurity is one of the most important challenges facing our economy and nation. To examine cybersecurity from both the legal business and national security perspectives, the ABA created the Cybersecurity Legal Task Force. The association asked the Task Force to address the tough questions about the appropriate role

and responsibility of lawyers in cyber-related incidents and to examine ways that lawyers and businesses can protect their practices and their clients’ confidential information and intellectual property.

The handbook was organized by Jill D. Rhodes and Vincent I. Polley,⁵ who wrote the first chapter and collected materials from a number of widely recognized experts within the ABA. Polley practiced law in Texas for many years as “deputy general counsel to Schlumberger Limited, where (inter alia) he coordinated cybersecurity defense planning, protecting the company’s trove of international oilfield data repositories from then nascent state-actor intrusion.”

The handbook provides excellent information about and insight into cyberissues. It could easily become a best-seller for the ABA given the increasing number of connected devices used to practice law as well as the importance of lawyers’ obligations to protect themselves and clients.

HOW BIG IS THE CYBERRISK?

An additional important source of information is the 2013 Data Breach Investigations Report from Verizon.⁶ The DBIR explains that the motives of cyberthreats include “money-minded miscreants [who] continued to cash in on low-hanging fruit from any tree within reach.”

Verizon published the DBIR with 19 cross-platform partners. The DBIR includes 20 Critical Security Controls that all lawyers (and clients) can use to focus on protecting their law practices and client data:

1. Inventory of authorized and unauthorized devices.
2. Inventory of authorized and unauthorized software, monitoring and notifications regarding unapproved software, application whitelisting, and software identification tagging.
3. Secure configurations for hardware and software on laptops, workstations, and servers.
4. Continuous vulnerability assessment and remediation, including automated vulnerability scanning, port checking, and patch management solutions.
5. Malware defenses, including anti-virus tools, disabling auto-run, traffic analysis, secure email usage, and sandboxing.
6. Application software security through testing and code review.
7. Wireless device identifiers and network access control.
8. Data recovery capability.
9. Security skills assessment and appropriate training to fill gaps.

10. Secure configurations and strong authentication for network devices such as firewalls, routers, and switches.
11. Limitations and control of network ports, protocols, and services, including conservative device configuration and default-deny stance.
12. Controlled use of administrative privileges, including identification and monitoring of administrative accounts, restriction of access to administrative accounts, and securing administrative accounts with strong authentication.
13. Boundary defense, including ingress and egress filtering based on blacklists and default-deny principle, DMZ traffic monitoring, IDS technologies, and application proxies.
14. Maintenance, monitoring, and analysis of security audit logs.
15. Controlled access based on the need to know through network segmentation and logical access control.
16. Account monitoring and control, including account auditing, password parameters, account lockout settings, monitoring attempts to access disabled accounts, and atypical account usage.
17. Data loss prevention by employing mobile hard drive encryption and DLP software.

18. Incident response and management.
19. Secure network engineering through network segmentation and establishment of security zones.
20. Penetration tests and red team exercises, including social attacks in sanctioned penetration testing.

If lawyers do not understand these 20 Critical Security Controls, it is time they started working with technology professionals who can help them and their clients. My hope is that this article will serve as a good starting point. **TBJ**

NOTES

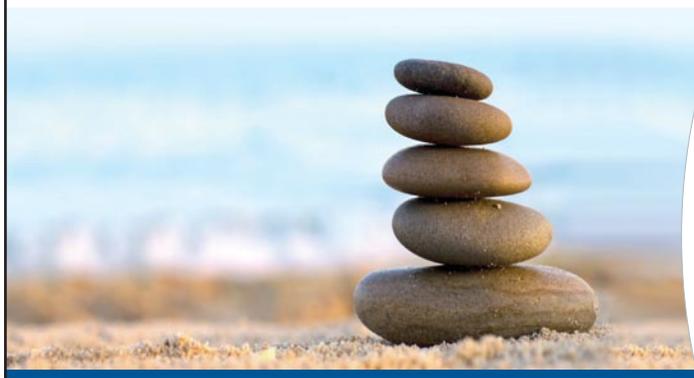
1. <http://mcaf.ee/utjz4>.
2. <http://www.verisign.com/ssl/ssl-information-center/ssl-resources/whitepaper-protect-sidejacking.pdf>.
3. <http://www.verizonenterprise.com/products/security/identity/ssl/>.
4. <http://apps.americanbar.org/abastore/index.cfm?pid=3550023§ion=main&fm=Product.AddToCart>.
5. www.knowconnect.com.
6. <http://www.verizonenterprise.com/DBIR/2013/>.



PETER S. VOGEL

is a trial partner, special master, and arbitrator at Gardere Wynne Sewell. Before practicing law, he worked as a computer programmer, received a master's degree in computer science, and taught graduate courses in information systems. Vogel has had trials around the U.S. on software implementations, misappropriation of trade secrets, copyright infringement, software patent infringement, and Internet disputes. For more information, go to vogel@itlawblog.com.

**WE'VE SPENT THE PAST 50 YEARS
PLANNING FOR RETIREMENT.
WHEN DID YOU START PLANNING?**



Planning for retirement requires forethought, perception, and a little patience. That's why the American Bar Association created the **ABA RETIREMENT FUNDS PROGRAM** – a comprehensive and affordable retirement plan built exclusively to address the unique needs of the legal community.

Call an ABA Retirement Funds Program
Regional Representative today!
(866) 812-1510 | www.abaretirement.com
joinus@abaretirement.com

The Program is available through the State Bar of Texas as a member benefit. This communication shall not constitute an offer to sell or the solicitation of an offer to buy, or a request of the recipient to indicate an interest in, and is not a recommendation of any security. Securities offered through ING Financial Advisers, LLC (Member SIPC). The ABA Retirement Funds Program and ING Financial Advisers, LLC, are separate, unaffiliated companies and are not responsible for one another's products and services.



State Bar of Texas members are eligible whether or not they are members of the American Bar Association.



CN0311-8585-0415