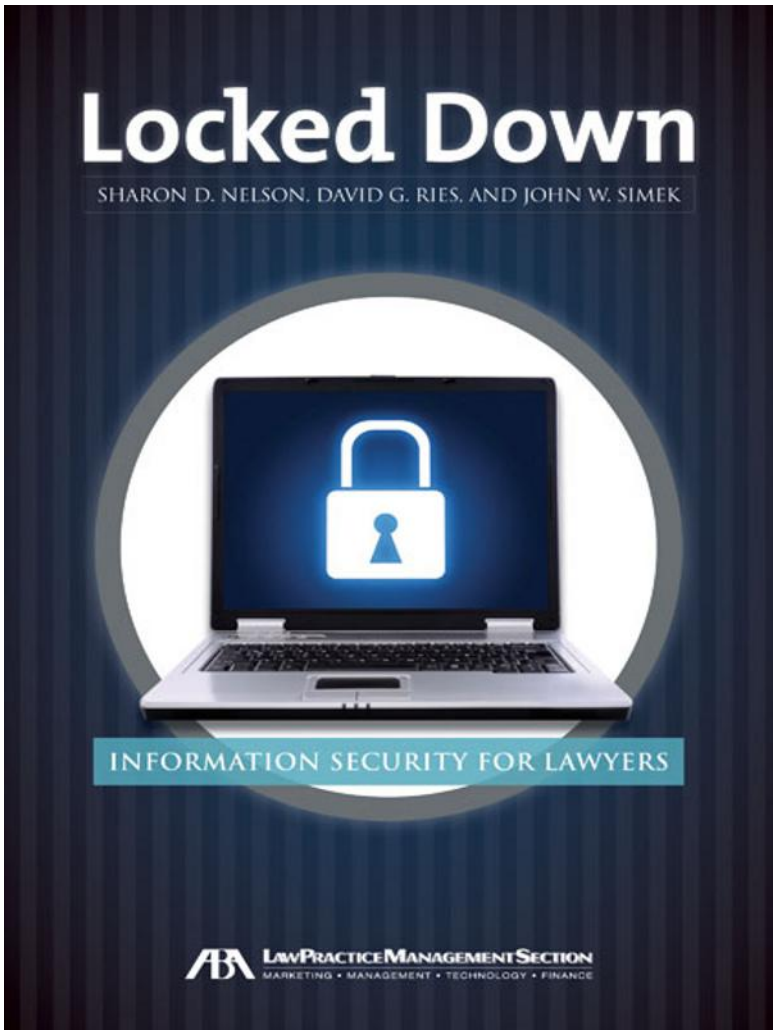
Locked Down
SHARON D. NELSON, DAVID G. RIES, AND JOHN W. SIMEK
INFORMATION SECURITY FOR LAWYERS
ABA LAW PRACTICE MANAGEMENT SECTION
MARKETING • MANAGEMENT • TECHNOLOGY • FINANCE

Locked Down

SHARON D. NELSON, DAVID G. RIES, AND JOHN W. SIMEK

ABA LAW PRACTICE MANAGEMENT SECTION
MARKETING • MANAGEMENT • TECHNOLOGY • FINANCE

Commitment to Quality: The Law Practice Management Section is committed to quality in our publications. Our authors are experienced practitioners in their fields. Prior to publication, the contents of all our books are rigorously reviewed by experts to ensure the highest quality product and presentation. Because we are committed to serving our readers' needs, we welcome your feedback on how we can improve future editions of this book.

Cover design by RIPE Creative, Inc.

The Law Practice Management Section of the American Bar Association offers an educational program for lawyers in practice. Books and other materials are published in furtherance of that program. Authors and editors of publications may express their own legal interpretations and opinions, which are not necessarily those of either the American Bar Association or the Law Practice Management Section unless adopted pursuant to the bylaws of the Association. The opinions expressed do not reflect in any way a position of the Section or the American Bar Association, nor do the positions of the Section or the American Bar Association necessarily reflect the opinions of the author.

Printed in the United States of America.

16 15 14 13 12 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Nelson, Sharon D.
Locked down: information security for law firms / Sharon D. Nelson, David G. Ries and John W. Simek.
p. cm.

Includes index.
ISBN 978-1-61438-364-2
1. Law offices—Computer networks—Security measures—United States. I. Ries, David G., 1949-II. Simek, John W. III. American Bar Association. Section of Law Practice Management. IV. Title.
KF320.A9N45 2012
340.068’4—dc23

2012007683

Discounts are available for books ordered in bulk. Special consideration is given to state bars, CLE programs, and other bar-related organizations. Inquire at Book Publishing, American Bar Association, 321 North Clark Street, Chicago, Illinois 60654-7598.

www.ShopABA.org

Dedication

AUTHORS NELSON AND SIMEK dedicate this book to our ever-growing family, having enjoyed two weddings last year and the addition of two grandchildren to our family. With great love, we dedicate this book to Kelly and Jeff Ameen, JJ and Sarah Simek, Sara and Rob Singmaster, Jason and Natalia Simek, Kim and Chris Haught and Jamie Simek as well as grandchildren Samantha and Jordan.

Author Dave Ries dedicates this book to his wife, Debbie, Dave Jr. and Jenelle Ries, my granddaughter Ellie, and Chris and Liz Ries. Their love and support have made this book and much more possible.

About the Authors

Sharon D. Nelson, Esq.

Sharon D. Nelson is the President of Sensei Enterprises, Inc. Ms. Nelson graduated from Georgetown University Law Center in 1978 and has been in private practice ever since. She now focuses exclusively on electronic evidence and information security law.

Ms. Nelson and Mr. Simek are the coeditors of the Internet law and technology newsletter *Bytes in Brief*. Ms. Nelson, Mr. Simek and their Sensei colleague Maschke are the coauthors of the 2008, 2009, 2010, 2011 and 2012 editions of *The Solo and Small Firm Legal Technology Guide: Critical Decisions Made Simple*. Ms. Nelson and Mr. Simek are also coauthors of *Information Security for Lawyers and Law Firms* (American Bar Association 2006). Additionally, Ms. Nelson and Mr. Simek are coauthors of *The Electronic Evidence and Discovery Handbook: Forms, Checklists, and Guidelines* (ABA 2006). Ms. Nelson is a coauthor of *How Good Lawyers Survive Bad Times* (ABA 2009). Their articles have appeared in numerous national publications, and they frequently lecture throughout the country on electronic evidence and legal technology subjects.

Ms. Nelson and Mr. Simek are the hosts of the Legal Talk Network's *Digital Detectives* podcast, and Ms. Nelson is a cohost of the ABA's *The Digital Edge: Lawyers and Technology* podcast.

Ms. Nelson will become the Vice President of the Virginia State Bar in June 2012 and its 75th President in June 2013. She is the past President of the Fairfax Bar Association, a Director of the Fairfax Law Foundation, past Chair of the ABA's TECHSHOW Board and past Chair of the ABA's Law Practice Management Publishing Board. She currently serves on the Governing Council of the ABA's Law Practice Management Section and as the Chair of its Education Board. She serves as a member of the Sedona Conference and of EDRM. She is a graduate of Leadership Fairfax and serves on the Governing Council of the Virginia State Bar as well as on its Executive Committee. She is the Chair of the VSB's Unauthorized Practice of Law Committee and serves on both its Technology Committee and its Standing Committee on Finance. She also serves on the Virginia Supreme Court's Advisory Committee on Statewide E-filing. She is a member of the ABA, the Virginia Bar, the Virginia Bar Association, the Virginia Trial Lawyers Association, the Virginia Women Attorney Association, the Women's Alliance for Financial Education and the Fairfax Bar Association.

David G. Ries, Esq.

David G. Ries is a partner in the Pittsburgh office of Thorp Reed & Armstrong, LLP, where he practices in the areas of environmental, commercial and technology litigation. He has used computers in his practice since the early 1980s and chairs his firm's e-Discovery and Records Management Group. He served two terms as a member and Chair of a Hearing Committee for the Disciplinary Board of the Supreme Court of Pennsylvania. Dave received his J.D. from Boston College Law School in 1974 and his B.A. from Boston College in 1971.

He has represented clients in a variety of technology litigation matters, including major systems implementation cases, and has advised clients on a number of technology law issues such as information security and privacy compliance, hardware and software agreements, electronic payments, technology use policies, domain name disputes, electronic records management, response to computer intrusions and electronic contracting.

He is a member of the ABA Law Practice Management Section Council and a member of the ABA Section of Science and Technology's Information Security Committee. He served on the ABA TECHSHOW Planning Board from 2005 through 2008.

Dave has frequently spoken on ethics, legal technology and technology law issues for legal, academic and professional groups, including the American Bar Association, the Association of Corporate Counsel, the Energy & Mineral Law Foundation, the Pennsylvania Bar Institute, the Information Systems Security Association and Carnegie Mellon University. He recently wrote "Safeguarding Client Data—Your Ethical and Legal Obligations," *Law Practice Magazine* (July/August 2010). He is the editor of *e-Discovery*, 2nd ed. (PBI Press 2011) and is a contributing author to *Information Security: A Legal, Business and Technical Handbook*, 2nd ed. (American Bar Association 2011) and *Information Security for Lawyers and Law Firms* (American Bar Association 2006).

John W. Simek

John W. Simek is the Vice President of Sensei Enterprises, Inc. He is an EnCase Certified Examiner (EnCE) and a

nationally known testifying expert in the area of computer forensics.

Mr. Simek holds a degree in engineering from the United States Merchant Marine Academy and an M.B.A. in finance from Saint Joseph's University. After forming Sensei, he ended his more than 20-year affiliation with Mobil Oil Corporation, where he served as a Senior Technologist troubleshooting and designing Mobil's networks throughout the Western Hemisphere.

In addition to his EnCE designation, Mr. Simek is a Certified Handheld Examiner, a Certified Novell Engineer, Microsoft Certified Professional + Internet, Microsoft Certified Systems Engineer, NT-Certified Independent Professional and a Certified Internetwork Professional. He is also a member of the High Tech Crime Network, the Sedona Conference, the Fairfax Bar Association, the International Information Systems Forensics Association and the ABA. In addition to coauthoring the books cited in Ms. Nelson's biography, he also serves on the Magazine and Education Boards of the ABA's Law Practice Management Section. He currently provides information technology support to more than 250 area law firms, legal entities and corporations. He lectures on legal technology and electronic evidence subjects throughout the United States and Canada.

Acknowledgments

WE THANK SENSEI'S PARALEGAL, Jason Foltin, for assistance with research for this book.

We express our appreciation to Chris Ries, an Information Security Engineer with Carnegie Mellon University. Chris has made a number of helpful suggestions for this book and shared his security insights with us over the years.

We are forever in debt to Tim Johnson, the former Executive Editor of LPM Publishing, for encouraging all of our authorship efforts over the years. Tim, your ability to encourage and apply the rod as deadlines slip a bit is unparalleled. At least this time, we were "close" to the deadline we set. We appreciate your support and constant good nature.

Thanks to our fantastic Production Manager, Denise Constantine, and our Editorial Assistant, Kimia Shelby. We are delighted to be working with LPM's gifted new Marketing Director, Lindsay Dawson. As always, the Pub Board staff is a joy to work with and we thank our Project Manager Jeff Flax, an old friend and valued colleague, and Pub Board Chair Bill Henslee who has always given us his support and a great deal of encouragement.

Sharon Nelson
Dave Ries
John Simek

Introduction

INEVITABLY, WHEN WE LECTURE on information security to lawyers, they describe themselves as being scared—usually because they had no concept that there were so many bogeymen to be afraid of. Sometimes, lawyers are frightened into absolute inertia and simply leave data security to whomever provides their information technology (IT) support.

We embarked upon this book hoping to make security a little more approachable. There need to be some technical explanations of course, but we've tried to keep the technical stuff to a minimum so that the average attorney can genuinely understand the security demons that are out there and how to defend against them. Forewarned really is forearmed.

This is not a DIY sort of project, especially if you've suffered a security breach. We make no attempt in this book to document the myriad steps that a professional information security expert would take. Our objective is to teach the data security basics in language that can be readily understood by lawyers. If you're in over your head, you'll hear us advise you again and again to seek professional help. Even among those who called themselves experts, there is often a shocking knowledge shortfall or a failure to keep up with current developments, which happen with dizzying speed!

One of the greatest difficulties of information security is that it is a moving target. The landscape changes so quickly that last year's (and sometimes even yesterday's) knowledge is woefully inadequate to combat today's threats. "Eternal

vigilance" is absolutely required for those of us who deal with data security issues.

Still, there are guiding principles that remain largely the same. We have tried to break information security down into digestible segments, knowing that some attorneys will pick up this book with concrete questions about specific security areas. Common questions we hear include:

1. What constitutes a strong password today?
2. How do I secure my smartphone?
3. Do I need to encrypt my laptop?
4. Can I safely use my laptop at Starbucks?

If your interests are narrow, you should be able to find what you're looking for by scanning the Contents. We would urge lawyers, however, to take a broad interest in the security of data because they have, unlike the general public, a professional and ethical requirement to safeguard client data.

Although lawyers are all aware of ABA Model Rule 1.6 (and we have an entire chapter on an attorney's duties to safeguard confidential data), the trick is how to keep client data secure in the digital era. It isn't easy. The paper world was much simpler to lock down. Computer security is expensive—and it takes time to understand it—and you will never finish learning because threats and technology morph constantly.

Are lawyers abiding by their ethical duty to preserve client confidences? Our opinion is that many are not. Here are a few reasons we hold that opinion.

- Security expert Rob Lee, a noted lecturer from the security firm Mandiant, has reported to us that Mandiant spent approximately 10% of its time in 2010 investigating data breaches at law firms.

- Security expert Matt Kesner, who is in charge of information security at a major law firm, reports that his firm has been breached twice—and that he is aware that other law firms have suffered security breaches—and failed to report them to clients.
- We have never performed a security assessment at a law firm (or for that matter, at any kind of business) without finding severe vulnerabilities that needed to be addressed.

Why do many otherwise competent lawyers fail so miserably in their duty to maintain the confidentiality of client data? Here are some of the reasons.

- Ignorance—they simply need education.
- The "it can't happen here" mentality. This is flatly wrong. Even the FBI issued an advisory in 2009 that law firms were specifically being targeted by identity thieves and by those performing business espionage—much of it originating from China and state sponsored, though of course the Chinese government has vehemently denied involvement in such activities. Matt Kesner, mentioned earlier as an expert, reports that the Chinese don't bother using their "A-level" hackers to infiltrate law firms; their security is so bad that the rookie "C-level" squads are able to penetrate law firms.
- According to press reports, lawyers and law firms are considered "soft targets"; they have high value information that's well organized and frequently have weak security.
- It's expensive. And it is. Protecting the security of client data can present a big burden for solos and small law firms. This does not take away a lawyer's ethical duty, however, and it is one reason the authors lecture so often on computer security. Once a lawyer sees the most common vulnerabilities, he or she can take remedial steps—or engage an IT consultant to do those things that are beyond the lawyer's skill.

- The need for vigilance never stops. You cannot secure your data once and think you're finished; the rules of information security change on close to a daily basis. Certainly, someone in the firm needs to keep up with changes on a regular basis or the firm needs to engage a security consultant to do periodic reviews. The standard advice is that security assessments need to be done twice a year. While that is desirable, it is in our judgment mandatory that assessments be conducted at least annually.

In the paper world, keeping client data confidential was easy and cheap. In the digital era, abiding by this particular ethical rule is often hard and expensive, but it must be done. We hope this book takes some of the "hard" away and also helps lawyers understand how many inexpensive steps exist to protect data without breaking the bank.

Often, this subject seems so dense and unapproachable that lawyers have the Ostrich Effect and simply bury their heads in the sand. Brian Ahern of Ahern Insurance Brokerage reported in 2011 that law firms are ranked ninth in terms of organizations with the highest risk of cyberexposure. As previously mentioned, even the Federal Bureau of Investigation warned law firms in November 2009 that they were increasingly becoming the target of hackers.

In the American Bar Association's 2011 Technology Survey, 21.1% of large law firms reported that their firm had experienced some sort of security breach, and 15% of all firms reported that they had suffered a security breach (Appendix A).

You would think that the magnitude of those numbers would be a wake-up call to the legal industry, but security always seems to take a backseat at law firms. In part, law firms are not used to budgeting for information security, and

yet that is clearly mandated in a world where technology rules us all. The crown jewels of law firms are their electronic files, and yet many law firms guard them sloppily.

For years, we've been warning lawyers that it's not a question of whether law firms will become victims of successful hacking attacks; rather, it's a matter of when. We pointed to incidents of dishonest insiders and lost or stolen laptops and portable media, but there were not disclosed incidents of successful hacking attacks. As the preceding examples show, we've now reached the "when," and attorneys and law firms need to address it.

We have set out in this book to provide practical advice in a condensed format. We hope that sharing some of the infosec "war stories" by way of examples will serve to make a business case for genuinely focusing on information security on a regular basis and, depending on the size of your firm and your area of practice, making sure that sufficient funds and time are allocated to protecting your firm's data.

CHAPTER ONE
Data Breach Nightmares and How to Prevent Them

Can Your Law Firm Be Breached?

In the paper world, it was remarkable when a law firm installed glass-breakage sensors on the windows of its 43rd-floor conference room, where documents were compiled for big cases and deals. The firm wanted to ensure that no one could rappel from the skyscraper's observation deck and break through the windows to steal the information. Boy oh boy, the times have really changed.

So now you've read in the introduction to this book that the FBI has warned law firms that they are targets for hackers and that security firm Mandiant has been spending 10% of its time investigating data breaches in law firms. In fact, Mandiant has confirmed that it has worked with more than 50 law firms dealing with confirmed or suspected data breaches. Clearly, it can happen to any firm.

Now consider the fact that most lawyers do not have cyberinsurance that will cover the expense of complying with data breach laws, which now exist in 46 states, the District of Columbia and the Virgin Islands. A single data breach could be a financial disaster for a small law firm.

The last stumbling block for lawyers who are disinclined to focus on security issues is their belief that it won't happen to

them—particularly their belief that no one would be interested in their data. Most of us can understand why merger and acquisition firms would be magnets for hackers; clearly, there is a great deal of money to be made on Wall Street with insider information.

Fewer people think about the money to be made by having an insider's knowledge of litigation, particularly in large suits involving a major corporation, where the result is likely to influence the stock market.

But what about small law firms? What attractive data do they hold? Many small firms practice family law, and their computers contain Social Security numbers, birth dates, and credit card and other detailed financial information. This is precisely the kind of data that identity thieves are looking for. They routinely scan for vulnerable systems seeking such data.

Business espionage is another motivation for breaking into law firms. Perhaps you represent a company and a competitor wishes to acquire business intelligence from you.

There is also the press. In 2011, the *News of the World* notoriously hacked into cell phones to feed the public's insatiable appetite for gossip. Consider all the interest in a murder trial—is it conceivable that a reporter might seek private information to get a scoop? Of course.

Need More Convincing?

Take a look at the Privacy Rights Clearinghouse web site's Chronology of Data Breaches from 2005 (when the first big breaches were disclosed) to the present. It may be found at **http://www.privacyrights.org/data-breach** and there are very sophisticated ways to sort the information.

Those were not the first large data breaches. They were disclosed because of a new California law that required

breach notification. Business executives acknowledged in congressional hearings that there had been breaches in the past, but they were not disclosed because there was no requirement to do so and it was not in their business interest to make the breaches public. As of mid-December 2011, the Clearinghouse reported 535 breaches involving 30.4 million sensitive records.

The first thing you'll note is that there are *lots* of data breaches each month. The second point you'll note is that you don't see a lot of law firms there. It is an open secret that law firms have played breaches very close to the vest and demand strict confidentiality agreements from information security vendors who investigate any compromise of their networks. This means, of course, that there probably are law firms out there that have chosen not to comply with state data breach notification laws, which frankly doesn't surprise us.

The third thing you'll notice is that there are a ton of health industry breaches here. Why? Because there is a federal law requiring that this industry report breaches, and the law has teeth. The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, contains several significant changes to the privacy rules in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HITECH requires that covered entities subject to the HIPAA privacy rule and their business associates must provide notice when unencrypted protected health information has been breached.

In spite of the law and the number of breaches you see reported, a study by the Healthcare Information and Management Systems Society found that only 17% of medical practices are likely to report an incident of medical

identity theft—in spite of all the federal and state laws requiring a report.

If a federal law is passed that covers personal information generally and provides stiff penalties, you'll be seeing a lot more industries in the Chronology of Data Breaches—and you'll probably find that law firms, always seeking to keep embarrassing information private, may well be like the medical practices and take their chances with flouting the law if they think they can "keep the lid on."

What's New in the Data Breach World?

The Ponemon Institute's 2011 "Cost of a Data Breach" study found that data breaches cost organizations $7.2 million on average in 2010. While this is a dreadfully high number, bear in mind that many of the data breaches that are reported are breaches that have gone public, some of them involuntarily, and they tend to involve very large corporations which are far more likely to report breaches than smaller entities.

With respect to smaller businesses, the National Small Business Cyber-security Study, published in 2011, reported that almost one-fifth of small businesses don't have or use antivirus software. Three-fifths don't use any encryption on their wireless networks, and two-thirds have no security plan whatever.

Security software behemoth Symantec revealed in September 2011 the results of its Small and Medium Business Threat Awareness Survey, and the numbers were disturbing. It surveyed 1,900 businesses worldwide with 5,499 employees. The key findings indicated that at least half of

these businesses continue to believe, in spite of all the evidence to the contrary, that they are not targets for cybercriminals; therefore, they are not taking actions to secure their data.

Another 2011 Ponemon study showed that 90% of businesses of all sizes reported a security breach in the preceding year. The majority had multiple breaches. It was striking that the majority didn't have much faith that they could stop breaches in the future; according to 77% of these businesses, the attacks were more sophisticated and severe.

IBM published its X-Force® 2011 Mid-year Trend and Risk Report in September 2011. Here are some of the more notable findings.

- Political hacktivism, first noted widely in 2010, is on the rise again in 2011, with hackers who have political objectives in mind. The hacker group Anonymous is a prime example.
- Attackers are becoming more sophisticated, developing better and better tools. They study their targets and wait for the right moment to try to enter high-value networks.
- America (no surprise) experienced an unprecedented number of high-profile data breaches in the first half of 2011, including Sony, Epsilon, HB Gary, Citigroup, Northrop Grumman, Booz Allen Hamilton and RSA.
- Mobile vulnerabilities and malware continue to soar and were predicted to double by the end of 2011. A Deloitte poll of 1,200 executives revealed that 28.4% believe they have unauthorized devices on their networks and almost 87% believe their companies are at risk for a cyberattack originating from a mobile device.
- Critical software vulnerabilities have tripled since 2010, with 7,000 vulnerabilities expected to be revealed by the end of 2011.

- Companies are beginning to ask themselves not “could it happen?” but “when it happens, how will we respond?”
- We are seeing a continuing rise in what are known as “advanced persistent threats” (APTs)—sometimes very complex—and after they compromise a network, they often go undiscovered for months.
- APTs (and this term is often too loosely used when the attack is conventional) typically cannot be defended by keeping patches current and running commercial security products. These attacks are specifically targeted as a rule and often exhibit careful long-term planning, also often using brand new vulnerabilities and obfuscation techniques.
- With APTs, it is sometimes advisable to let the attack continue while you document it and run counterintelligence on it. Forensic analysis is going to be a key activity, adding to the inevitable financial burden.
- In spite of the fact that we know a great deal about how to protect ourselves from things like SQL injections, we simply aren’t doing it. For those who were wondering, SQL injection is a code injection technique that exploits a security vulnerability in a web site’s software.

A new development in 2011 was e-mails that appear to come from your printer, scanner or all-in-one device. They are a form of attack, using e-mails with false header information to get users to click on the link contained in the e-mail. Author Nelson got one as she was writing this chapter. Here’s what it looked like.

From: support@senseient.com
[mailto:support@senseient.com]
Sent: Thursday, December 01, 2011 3:21 AM
To: Sharon D. Nelson

Subject: Re: Fwd: Re: Scan from a Xerox W. Pro #6979530
A Document was scanned and sent to you using a Xerox Work-
Centre OF986646.
Sent by: KARINA
Image(s): 3
Type: Image View (this part was hyperlinked)
Device: XER077KD1S342079
3e12afb0-4d5c6789

This wasn't a good scam because she knows her company doesn't have this kind of device—and no KARINA works with her. But there are more sophisticated versions of these attacks, so beware of the new demon in town.

Verizon's 2011 Data Breach report noted that, in 2010, the Secret Service arrested more than 1,200 suspects for cybercrimes. The investigations involved more than $500 million in fraud losses.

Verizon also identified only 16% of the threats as coming from internal sources, with 92% coming from external sources and less than 1% coming from third parties who had a relationship with the breached entity.

Where do these external threats come from? Sixty-five percent come from Eastern Europe, which is notorious for cybercrime (and where many investigations "go to die"), 19% from North America, and 6% from South and Southeast Asia. Those are the top three culprits.

The leading three threat agents are hacking, malware and exploitation of physical security vulnerabilities, followed by the misuse of data to which someone had access, and social engineering.

While insider threats appear to be down, bear in mind the case of Matthew Kluger, a lawyer who allegedly stole insider