THE BIG BREACH

Data breaches have become one of the most serious threats to any business, with cyber criminals on the prowl 24 hours a day. If your firm is not on top of IT security, you never know who might be able to infiltrate your information systems and steal your firm's (and your clients') sensitive information.

Check out numbers that illustrate this menacing risk to your firm.

DATA SECURITY IS AN URGENT BUSINESS CONCERN FOR LAW FIRMS

The **FBI'S CYBER DIVISION** issued a Private Industry Notification in March 2016, warning of technically proficient hackers seeking to gain sustained access to the networks of multiple international law firms.[1]

SIXTY-SIX PERCENT of U.S. law firms reported some level of data breach in 2016, with varying levels of compromise involved.[2]

Hacking attempts were made on **OVER 200** U.S. law firms between 2016 and 2017, **40 PERCENT** of which didn't even know that they had been breached.[3]

APPROXIMATELY 40 PERCENT of law firms that experienced a data breach reported significant resulting business downtime and loss of billable hours, and **ONE IN SIX** reported loss of important files and information.[4]

Nearly **ONE-THIRD** of law firms have not undertaken a formal information, security and privacy assessment and **47 PERCENT** of law firms say they do not regularly test their cybersecurity programs.[5]

CYBERSECURITY IS INCREASINGLY TOP OF MIND FOR CORPORATE COUNSEL

A 2017 survey found that **72 PERCENT** of corporate legal departments point to cyber threats as their top priority risk issue today, ahead of FCPA compliance, international agreements and other risk management challenges.[6]

SEVENTY-EIGHT PERCENT of IT administrators report two or more data security threats in 2017 and **68 PERCENT** report the same threat occurring multiple times.[7]

Corporate victims of data breaches are spread out across the economic landscape. The most commonly targeted industries are:

24	15	15	12
FINANCE	HEALTHCARE	RETAIL / ACCOMODATION	PUBLIC SECTOR

NINETY-FIVE of corporate counsel believe that cybersecurity breaches are becoming more frequent in their industries and **27 PERCENT** of corporate counsel say their companies do not regularly test their cybersecurity programs.[8]

American businesses are projected to lose **$3 TRILLION** to cybercrime in 2020, up from **$1 TRILLION** in 2016.[10]

Global spending on cybersecurity is projected to increase to **$96.3 BILLION** in 2018, an increase of **8 PERCENT** from 2017.

41 PERCENT of U.S. lawyers said that their law firm or company plans to increase spending on cybersecurity-related tools and services within the next 12 months.

LEGAL PROFESSIONALS ARE RESPONDING TO THE THREAT

Two-thirds of chief legal officers and general counsel ranked protection against data breaches as "very" or "extremely" important in 2017, leading the Association of Corporate Counsel to issue guidelines for law firm cybersecurity measures.[11]

Worldwide spending on cybersecurity is predicted to top $1 trillion for the five-year period from 2017 to 2021, at a 12-to-15 percent annual growth rate in corporate cybersecurity investments.[12]

Roughly 32 percent of companies purchased some form of cyber liability and / or data breach coverage in 2017 and 44 percent increased their coverage levels from a year ago.[13]

Thirty-eight percent of law firms have created a disaster recovery / business continuity plan.[14]

Thirty-four percent of law firms said they purchased cloud storage in 2016 and another 25 percent said they planned to purchase more cloud storage solutions over the next year.[15]

6-STEP CHECKLIST FOR BUILDING A DATA SECURITY PLAN

1. **CREATE WRITTEN POLICIES**, based on standards such as ISO 27002, and secure buy-in from your executive team so these policies are reinforced. Schedule regular training sessions for anyone in the firm who is involved with data management in order to maximize security awareness among your employees.
2. **INVENTORY YOUR INFORMATION SYSTEMS** so you have a detailed record of exactly what the firm has in its purview and where all of the controls / permissions are located.
3. **IMPLEMENT ACCESS CONTROLS** on a "need to know" basis so that employees only have credentials to get into the files that relate to their job functions and then segment your systems so that specific IT pieces that do not need to be connected to highly sensitive client data are not inadvertently connected.
4. **KEEP YOUR SYSTEMS UP TO DATE** with the most recent software patches, including antivirus software. It is crucial to keep your firm's IT armor updated in order to reduce the attack surface available to criminal hackers.
5. **CONDUCT ANNUAL THIRD-PARTY RISK ASSESSMENTS** to validate your vendors. Make sure to establish managed services agreements that cover security and privacy expectations, and then regularly assess your vendors' security protocols to determine what specific data you will allow them to process, access or host.
6. **HAVE AN INCIDENT RESPONSE PLAN** in place so the firm is "breach ready" on a 24/7/365 basis. The last thing you want to be doing is guessing how to respond when that dreaded cyberattack occurs. Also, check your liability / cybersecurity insurance policies on an annual basis so that your policy coverages remain comprehensive and adequate for the firm's risk exposure.

Managed Technology Services LLC (MTS), an HBR Consulting and LexisNexis solution, is a trusted data-hosting service provider to the legal industry. For more than a decade, MTS experts have collaborated with clients – including 25 percent of the Am Law 100 – to manage infrastructure, systems performance, cost and risk.

For more information, please visit hbrlegalmts.com.

MANAGED TECHNOLOGY SERVICES
an HBR Consulting + LexisNexis solution

SOURCES
[1]https://www.bankinfosecurity.com/law-firms-under-fire-a-9026 https://www.helpnetsecurity.com/2017/07/06/law-firms-data-breach/
[2]https://www.logicforce.com/reports/detail/cyber-security-q1
[3]https://www.americanbar.org/publications/litigation-news/featured-articles/2017/law-firm-cybersecurity-breach-opens-door-to-lawsuit.html
[4]https://www.alm.com/press_release/cybersecurity-ignorance-is-big-risk-for-law-firms-corporate-counsel-alm-legal-intelligence-analysts-find/
[5]https://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/2017/Cybersecurity-top-concern-of-corporate-counsel.ashx
[6]https://www.sans.org/reading-room/whitepapers/threats/sensitive-data-risk-2017-data-protection-survey-37900
[7]http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[8]https://www.alm.com/press_release/cybersecurity-ignorance-is-big-risk-for-law-firms-corporate-counsel-alm-legal-intelligence-analysts-find/
[9]https://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/2017/Cybersecurity-top-concern-of-corporate-counsel.ashx
[10]https://www.sec.com/about/securitiesexchangecommission/subdocuments/cybersecurityguidelines.cfm
[11]https://www.csoonline.com/article/3083795/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html
[12]https://www.cialr.com/resources/cyber-market-survey-spring-2017/
[13]https://www.lexactpinvacy.com/law-firm-cybersecurity-an-industry-at-serious-risk/
[14]http://insidelegal.typepad.com/files/2016_ILTA_InsideLegal_Technology_Purchasing_Survey.pdf
[15]https://www.law.com/legaltechnews/sites/legaltechnews/2017/12/27/cybersecurity-spending-at-law-firms-legal-departments-is-predicted-to-increase-in-2018/