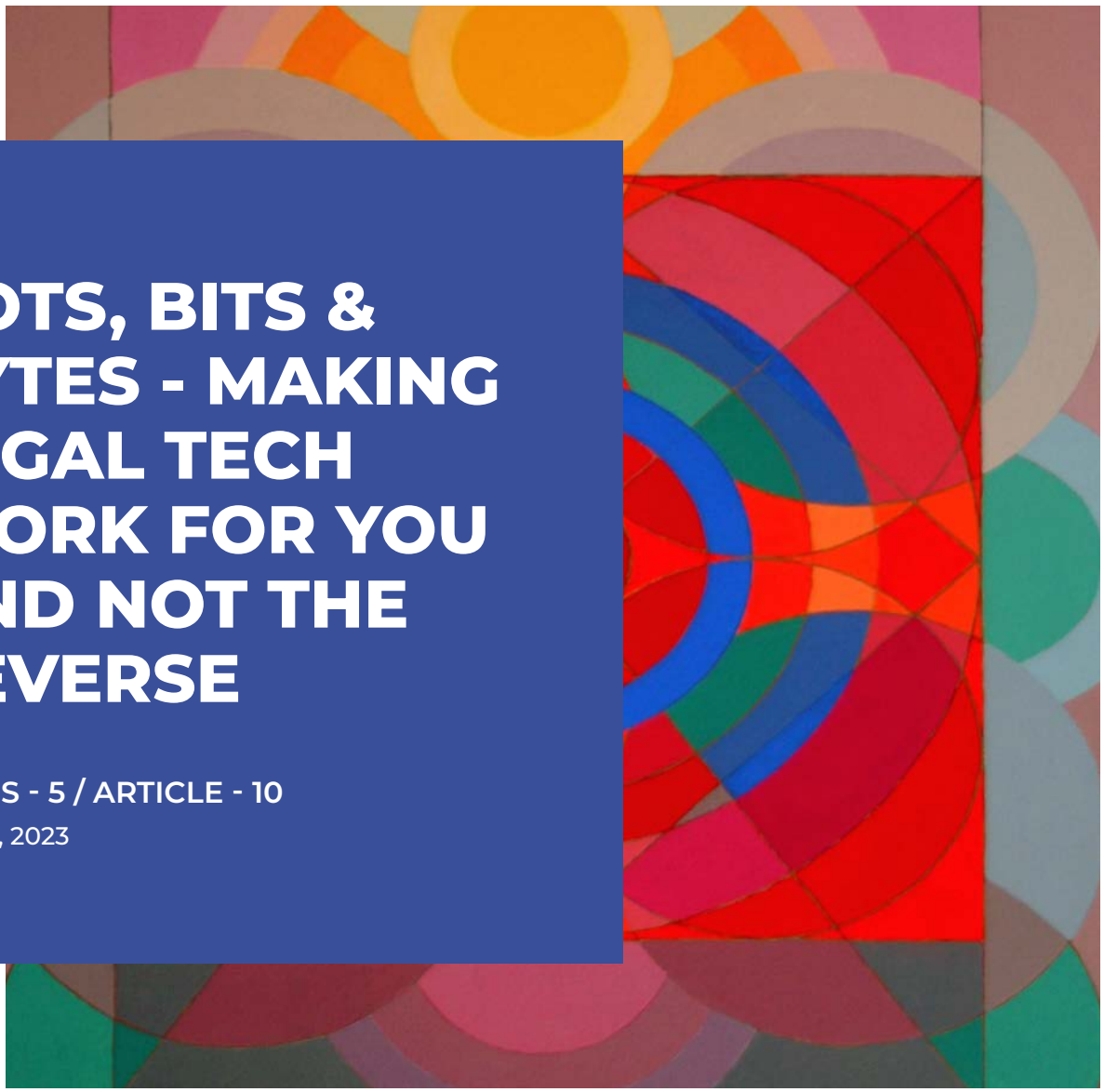
DATA LOSS RISK AND REMOTE WORK ARRANGEMENTS



BOTS, BITS & BYTES - MAKING LEGAL TECH WORK FOR YOU AND NOT THE REVERSE

SERIES - 5 / ARTICLE - 10

MAY 31, 2023

By **Jeffrey Brochin, Esq.**

GreenPoint> Law&Compliance

william.anderson@greenpointglobal.com | pranav.menon@greenpointglobal.com

International Corporate Center, 555 Theodore Fremd Avenue, Suite A102 Rye, NY 10580

www.greenpointlegal.com

Clearly, the COVID-19 pandemic made a paradigm shift in the way—and more specifically, in the place where—employees perform their work. Although there were expectations that after the end of the pandemic, workplace arrangements would get 'back to normal', few anticipated that the newly inaugurated, widespread, remote-work arrangements would themselves become the new 'normal'. The post-pandemic reality is that today, just under 60% of employees who have the work-from-home option for part or all of their work have opted to do so, as opposed to just 23% of employees taking that option prior to the pandemic. A natural by-product of the remote work arrangement has been an increase in information shared via home networks and a blurring of the lines between personal versus work devices and work environments. Sensitive business information has not only become more vulnerable but, in fact, more often compromised. We will examine the increased data loss risk brought on by the newfound remote work arrangements.

BYOD and Risk

In some cases, the employer provides all of the hardware that an employee will need in order to work from home; but in other cases, the employer depends upon the employee to use his or her own equipment ('Bring Your Own Device') whether that means, desktop computers, laptops, printers, or internet connectivity services and devices. Even where the employer supplies the employee's computer, that still oftentimes leaves the weak link of an unsecured home WI-FI network as a serious data loss vulnerability.

Although IT managers at the workplace can usually stop scammers before the material reaches company computers through the installation of sophisticated firewalls and other protections, employees working at home are more likely to be scammed by innocent-looking social engineering scams, thereby allowing data risk not just to their own family data, but also that of their employer. In fact, in 2021, there was a 270% increase in 'social engineering' occurrences including email phishing, phone calls (vishing) and text (smishing) scams. Phishing attacks alone were up by over 50% that year.

Failure to Update

Data loss analysts have also determined that although workers onsite are more disciplined in adhering to strict security protocols, remote workers tend to be more lax aboutsuch safeguards. In addition, the employer likely keeps all apps updated so as to further protect against cybersecurity threats, whereas home workers infrequently respond to update notifications in a timely manner. Research has shown that 36% of remote workers delay installing software updates, and a mere 34% acknowledged that they properly adhere to company cybersecurity guidelines.

The combination of unsecured home networks and out-of-date software creates exposed gateways for cybercriminals to access personal and also company networks.

Who and What Are the Targets?

Research conducted by proxy server provider, Proxyrack, determined that the United States (perhaps not surprisingly) is the number one most-targeted country for data breaches, with an incident rate of 7,221,177 per million

"THE PANDEMIC — AND THE REALITY OF MANY EMPLOYEES WORKING FROM HOME — HAS ADDED A NEW LEVEL OF COMPLEXITY AROUND DATA LOSS PROTECTION, REGULATORY COMPLIANCE, AND GOVERNANCE. EMPLOYEES ARE WORKING IN LESS SECURE AND CONTROLLED ENVIRONMENTS, OFTEN CLOSE TO FAMILY MEMBERS OR ROOMMATES, AND WORKING MORE FLUIDLY ACROSS MULTIPLE COMMUNICATION CHANNELS. EVEN THE MOST WELL-INTENTIONED PROFESSIONALS ARE LIKELY TO BE MORE PRONE TO POTENTIAL COMPLIANCE BREACHES."

—Reshma Khamis, Bloomberg Vault Product Manager

people. The U.S. is followed by the 'Middle East', with UAE and Saudi Arabia being the most targeted in that region and Canada landing in the number three spot.

As to industries affected, the healthcare sector is far and away the most targeted industry, followed by the financial sector and then pharmaceuticals. Healthcare data breaches cost an average of $9.23 million, the highest figure among any industry surveyed, and in the financial sector, data breaches cost an average of $5.27 million. But beyond the adverse financial impact, data loss also results in reputational damage with loss of customer confidence and loyalty, thereby also hurting the compromised company in the marketplace.

Seeking Remedies

So, in an era of increased remote work arrangements and the concomitant increased risk of data loss, is there anything an organization can do to eliminate or at least mitigate the loss? Experts point to several steps that, in combination, can greatly reduce data loss arising from remote work arrangements:

Data Governance:
Implementing and enforcing data governance rules and protocols is essential to addressing cybersecurity weaknesses. Employees must be made aware of the company guidelines, and such devices as two-factor authentication and enhanced access permissions must be put in place.

Cybersecurity Training:
Employees working from home need to be trained in 'best practices' regarding the handling of confidential data. Among those best practices is the regularly scheduled change of password regimen.

Cloud Storage:
Both stored data and data operations should be cloud-based as a means of maintaining a cybersecure infrastructure that is not dependent upon individual devices, whether employee-owned or company-owned.

'Employing' AI

Lastly, regardless of whether employees are onsite or working remotely, investment in the latest technology to protect against the latest threats cannot be overemphasized. Hackers, ransomware criminals, and other culprits have at their disposal the training and the tools to wreak havoc with your organization's data. According to a 2022 study conducted by IBM and the Ponemon Institute, organizations with fully deployed security AI automation experienced an average data breach loss decrease of $2.90 million, and the duration of the breach was also reduced, taking an average of 184 days to identify a breach and 63 days to contain it, compared to 239 days and 85 days respectively for non-automated systems.

By implementing the most up-to-date technology and software solutions, businesses can continue to benefit from the remote work cost advantages without suffering the increased risk of data loss.

Executive Summary

1. The Issue

How has the increase in remote work arrangements impacted the risk of data loss?

2. The Gravamen

The risk of data loss has increased dramatically as remote employees make use of less secure equipment and internet connections and thereby expose sensitive and confidential employer data to cybersecurity threats.

3. The Path Forward

Employing cybersecurity protocols for employees and investing in advanced cybersecurity technology for your organization's systems, regardless of location, can reduce the risk of data loss.

Action Items:

1 Data Governance:

If your organization does not already have in place sound data governance policies, the same must be instituted at once before offering remote work options to employees.

2 Enforcement of Guidelines:

Employees must be fully trained in such matters as who can use computers that are connected to your organization's system, and firm authentication protocols must be in place and enforced.

3 Authentication Credentials:

Aside from limiting who has access to sensitive information, even those with access granted must have two-factor authentication protocols in place, and a change-of-password monitors must force regular updates.

4 Off-device Storage:

Sensitive data should be stored on secure cloud servers and not on local devices, and certainly not on any employee-controlled device.

Further Readings

1. https://www.sontiq.com/resources/remote-work-data-breach/
2. https://www.workflowmax.com/blog/how-to-keep-your-data-safe-when-working-remotely
3. https://www.forbes.com/sites/benjaminlaker/2023/01/10/remote-working-increases-likelihood-of-data-breaches-says-research/
4. https://www.linkedin.com/pulse/how-remote-work-leading-more-data-breaches-than-ever-shelt/
5. https://www.iii.org/insuranceindustryblog/study-highlights-cost-of-data-breaches-in-a-remote-work-world/

Jeffrey Brochin, Esq.

GREENPOINT STAFF COUNSEL
AND CONTENT EDITOR

After receiving his Juris Doctor degree from The John Marshall Law School in Chicago, Mr. Brochin served as an Administrative Law Judge with the Illinois Department of Labor for six years where he presided over cases dealing with job separation issues and matters pertaining to contested Unemployment Insurance claims. He also co-wrote the agency's administrative rules, and periodically served as a 'ghost writer' for Board of Review decisions. Following that position, he was Director of Development for a Chicago-area non-profit college where he was responsible for High Net Worth donations to the institution. For the next eighteen years he practiced as a solo practitioner attorney with an emphasis in the fields of Real Estate law and Commercial Contracts transactions, and was an agent for several national title insurance agencies.

In 2003 he was recruited to head up a U.S. title insurance research office in Israel, a position he held for four years, and between 2007-2017 he participated in litigation support for several high-profile cases. He has taught Business Law as a faculty member of the Jerusalem College of Technology, and has authored a wide variety of legal White Papers and timely legal articles as a professional legal content writer for GPL clients. Separate from his legal writing, he has co-authored academic articles on Middle East security topics that have been published in peer-reviewed publications.

William H. Anderson, Esq.

MANAGING DIRECTOR AND HEAD OF
FINANCIAL PRODUCTS AND SERVICES

William Anderson is Managing Director and Head of Law & Compliance. He leads the GreenPoint practice in providing regulatory, legal, and technology solutions to law firms, legal publishers, and in-house law departments around the world, overseeing our team of experienced US attorneys and data and technology experts. Will has over 25 years' experience working with corporations to improve the management of their legal and corporate compliance functions. Will began his legal career as a litigator with a predecessor firm to Drinker, Biddle LLP. He then served as in-house counsel to Andersen Consulting LLP, managing risk and working with outside counsel on active litigation involving the firm.

Will has leveraged his legal experience interpreting regulations and appearing before federal (DOJ, SEC, FTC) and state agencies (NYAG) to oversee research and other areas at Bear Stearns. In this capacity, he counseled analysts on regulatory risk and evolving compliance requirements. Will also consulted on the development of a proprietary tool to ensure effective documentation of compliance clearance of research reports. Will then went on to work in product development and content creation for a global online compliance development firm pioneering the dynamic updating of regulated firms' policies and procedures from online updates and resources. Will holds a Juris Doctorate with High Honors from the Washington University School of Law in Saint Louis and is admitted to state and federal bars. He lives in Pawling, NY, with his wife and daughter.

Sanjay Sharma, PhD

FOUNDER AND CHAIRMAN

Pranav Menon, Esq.

LEGAL RECRUITMENT
MANAGER AND DATA
PRIVACY SPECIALIST – LAW
& COMPLIANCE | GPESR

GreenPoint> Law&Compliance

About GreenPoint Law & Compliance

- GreenPoint Global was founded in 2001 and since that time has faithfully served an expanding roster of clients. GreenPoint leverages a unique combination of US-trained attorneys and proprietary technology to deliver a unique offering of skill and flexibility to meet client needs.
- Our core team of experienced US attorneys is based in Israel and works US hours. The breadth of experience of our attorneys ensures high-quality, cost-effective results across a wide range of legal, compliance, and regulatory matters.
- GreenPoint's methodology and proven track record of achieving client objectives has resulted in a broad base of clients in the United States, ranging from Fortune 500 insurance companies to solo practitioners, law firms, in-house law departments, and legal publishers. GreenPoint attorneys are selectively recruited and deployed based on possessing demonstrable subject matter expertise covering a broad spectrum of substantive US laws and regulations. The work product of our attorneys is thoroughly vetted internally before delivery to client. Adherence to quality, value and flexibility is at the core of our foundation.

GreenPoint> Global

About GreenPoint Global

- GreenPoint Global provides litigation support, finance and technology solutions to insurers, law firms, banks, and in-house law departments through our subject matter experts and process specialists.
- Founded in 2001 and headquartered in Rye, New York, GreenPoint has grown to over 500 employees with a global footprint. We have a stable and growing client base that ranges from small and medium-sized organizations to Fortune 1000 companies worldwide. Our production and management teams are located in the US, India, and Israel with access to deep pools of subject matter experts. Our greatest strength is our employee-base of experienced lawyers, paralegals, process specialists, financial analysts, and software developers. We have leading edge software development capabilities with over 50 professionals on staff, working on internal and client projects.
- GreenPoint is certified by the TÜV SÜD (South Asia) for the highest standards of Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2013). GreenPoint is certified as a Minority and Woman Owned Business Enterprise (MWBE) by New York City and a Minority Owned Business Enterprise (MBE) by the State of New York. GreenPoint complies with all federal and state contracting requirements. GreenPoint is owned by its founders and principals and is debt free. For comprehensive information on our services and products under Law & Compliance and Finance, please visit our subsidiary websites through the division's menu.