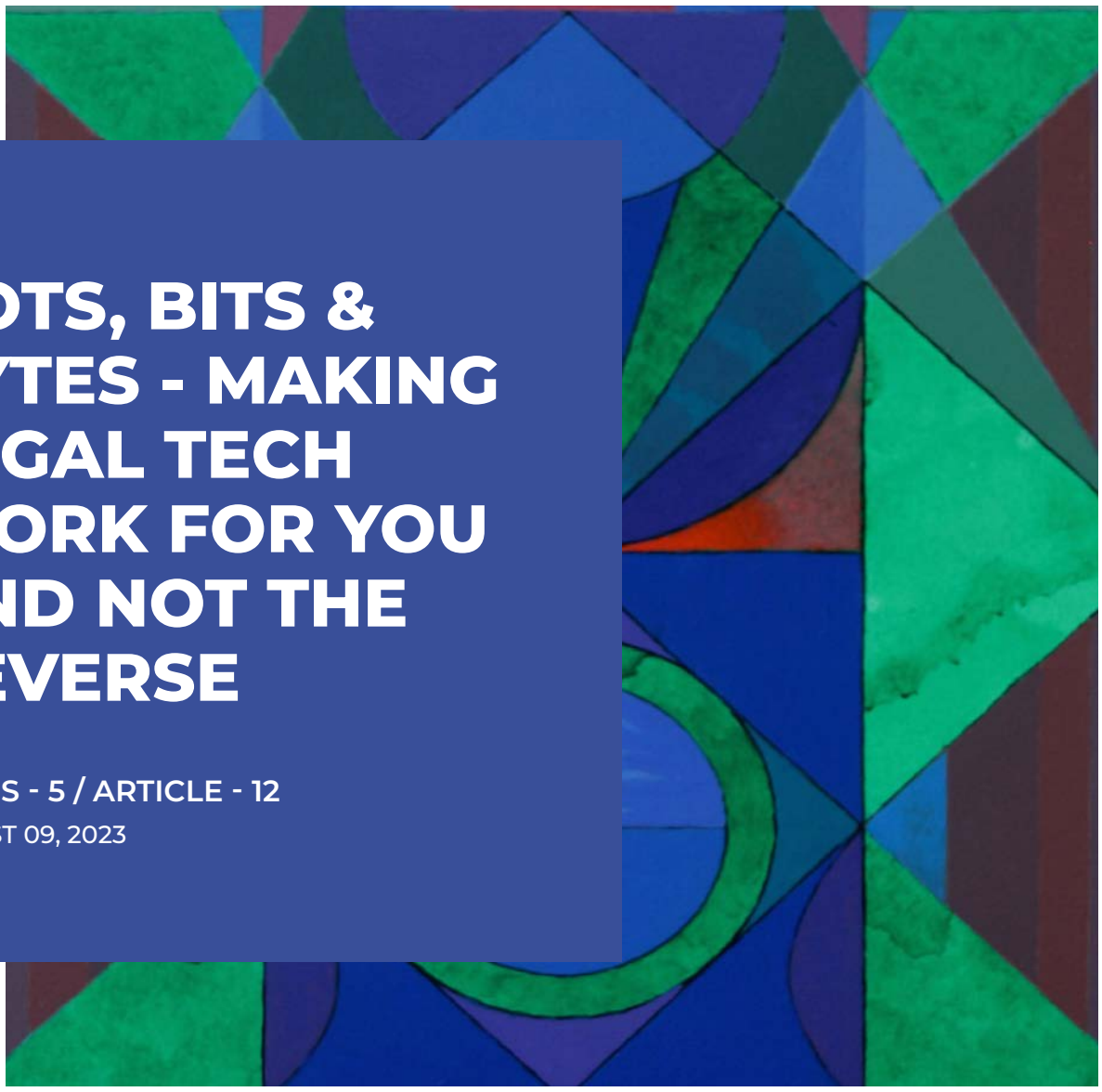
SMBs AND CYBER SECURITY



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

SERIES - 5 / ARTICLE - 12

AUGUST 09, 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

When you think of cyberattacks, highly-publicized breaches such as occurred at Twitter, Cash App, Nvidia, Uber, or Grand Theft Auto probably come to mind. But most small businesses (SMBs) presume that they are too small to be bothered with and therefore need to be concerned with protecting against cyberattacks. Unfortunately, that thinking is wrong—and quite costly. Statistically, about 46% of all cyberattacks carried out are against small businesses (fewer than 1,000 employees), and a huge 61% of all SMBs were the target of a cyberattack last year. It's time that SMBs took the threat seriously—and did something about it.

The Cost of SMB Cyberattacks

Some interesting statistics came out of a study conducted by IBM and the Ponemon Institute. To begin with, in 2020 alone, there were over 700,000 attacks against SMBs, costing them $2.8 billion in damages; malware was the most common type of cyberattack aimed at small businesses, with 83% of all ransomware attacks in 2021 being carried out against SMBs; and 51% of SMBs that suffered ransomware attacks ended up paying the attackers.

Furthermore, nearly 40% of SMBs reported that they lost crucial data as a result of an attack, and 75% reported that they could not continue operating if they were hit with ransomware. Given these numbers, one would think that SMBs would be the first to address the need for better cybersecurity, yet only recently have SMBs recognized the value of investing in the proper technology and adopting proper policies, and only 17% carry 'cyber insurance.'

The 'Soft Costs'' That Damage a Business

Aside from the fact that a cyber attacker can drain corporate bank accounts that are accessed—and even personal bank accounts that are accessible via business networks—there is also the issue of identity theft that oftentimes occurs along with cyberattacks. A company's employees can have their lives destroyed over such breaches. Customer's credit card information and other financial details affecting your customers can also be compromised, which, needless to say, can result in losing those customers in addition to dealing with the lawsuits they will likely bring.

Other ancillary damage includes the cost of bringing in cyber experts to investigate the matter, the costs of notifying customers of the breach (which also involves binging in professional consultants in order to be in compliance with all regulations that the business will now have to comply with), providing volumes of records to law enforcement, and an increase in liability insurance premiums. For investors, a data breach and its resultant losses to the company may be viewed as negligence and erode the confidence of investors in the SMB's management.

Creating a Recovery Plan

The impact of cybercrime on an SMB can be catastrophic, and some cybercrimes can even shutter a business permanently. According to many experts, staying ahead of the cyber curve requires that an SMB have in place a recovery plan or business continuity plan just as for any other sort of disaster. Your company should have incident response teams that include cyber experts so as to be able to quickly identify a breach, hopefully, limit its spread and impact, and restore services as quickly as possible.

"THE LARGE BUSINESSES CONTINUE TO INVEST IN THEIR CYBERSECURITY AND ENHANCE THEIR CYBERSECURITY POSTURE. SO WHAT THE CYBERCRIMINALS ARE DOING IS THEY'RE PIVOTING, THEY'RE EVOLVING AND TARGETING THE SOFT TARGETS, WHICH ARE THE SMALL AND MEDIUM BUSINESSES."

— Michael Sohn, FBI Supervisory Special Agent

Going forward, the team must analyze the breach to ensure that the business does not fall prey to cyber attackers in the future. Technically recovering from an attack is only one part of the response team's function, and smoothing out the accompanying havoc is another. The team will also need PR experts, whether outside consultants or in-house staff, to make sure that customers and the public receive accurate information and not online rumors.

FCC Tips for SMBs

Because the internet is the theater in which cyberattacks take place, cybersecurity is particularly within the purview of the FCC. And, due to the fact that the theft of digital information is now the most commonly reported fraud—eclipsing even physical theft—the agency has drafted guidance to assist SMBs in developing a culture of security so as to enhance both the SMBs' and their consumers' confidence. Among the FCC's tips for better cybersecurity are the following:

- Training employees in security principles. Basic security practices such as strong passwords and Internet use guidelines should be established for employees and reviewed on a regular basis, with rules in effect for enforcement.

- Protecting information, computers, and networks. 'Clean machines' having the latest security software, browser updates, and operating system updates are considered the best defenses against malware, viruses, and numerous other online threats. It is especially important for antivirus software scans to run automatically. important for antivirus software scans to run automatically.

- Firewalls. Preventing outside access is the job of a firewall, and this program is important to have installed on the equipment of remote workers as well.

- Company mobile devices. A frequently overlooked access point for cybercriminals is by way of mobile phones. Mobile devices pose a significant security challenge, especially if they hold confidential information or can access the corporate network. Mobile devices must be password protected and have data encrypted.

Advice from the FBI

While it is true that SMBs simply do not have the same level of resources as larger corporations to either fend off cyberattacks or mitigate their effects, SMBs can nevertheless do much with what they have to stay cyber-secure. Echoing the FCC's suggestions, FBI Supervisory Special Agent Michael Sohn recommended that SMBs practice 'cyber hygiene', noting that 'a lot of the cyberattacks that we have witnessed from our investigations, almost all of them could have been prevented by doing very basic cyber hygiene.' This includes using multi-factor or two-party authentication and not using the same password across multiple logins or accounts. Although this sounds very simple, the agency has witnessed many situations in which the same password used for an email might also be used for a payroll account or access to other financial accounts. Although utilizing a good password manager is not necessarily a 'silver bullet' to stop cyber attackers, that tool, along with other sound cybersecurity practices, can go a long way as a valuable layer in your SMB's data and financial protection.

Executive Summary

1. The Issue

How can SMBs stay ahead of the curve in fighting cyberattacks?

2. The Gravamen

By adopting basic cybersecurity practices—including up-to-date password management and policy enforcement—even smaller businesses can mitigate breach occurrences.

3. The Path Forward

A disaster response team should be organized to quickly recover operations in the event a cyberattack occurs.

Action Items:

1 Change of Mindset:

If you thought that cyberattacks mainly hit big companies, then to begin with, your managers need a sea change as to their perspective on this growing crisis.

2 Cybersecurity Policies:

Put in place cybersecurity policies covering everything from password practices, employee responses to suspicious emails, clicking on pop-ups, and overall use of company computers, and accessing company internet from mobile phones.

3 Disaster Response Team:

By having in place a team of professionals, including IT, PR, and a consultant, to address the compliance requirements following an attack, your company can at least limit the ancillary damage from an attack.

4 Technological Tools:

Don't ignore the technology that already exists to help protect your company, such as firewalls, regular security updates and patches, and server access authentication, which is a technology that even SMBs should be able to afford when scaled to their size.

Further Readings

1. https://www.cisa.gov/cyber-guidance-small-businesses
2. https://www.strongdm.com/blog/small-business-cyber-security-statistics
3. https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
4. https://www.cnbc.com/2022/12/16/fbi-7-billion-lost-in-criminal-hacks-most-victims-small-businesses.html
5. https://www.stickmancyber.com/cybersecurity-blog/impact-of-cyber-crime-on-business-cybercrime-business-continuity

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.