WHITE PAPER

Market Pulse

Getting Around User Workarounds: Security to Account for Human Nature

A recent IDG study finds that despite confidence in their security practices, legal firms are at high risk due to employee actions.

It's worse than you might think: 79% of IT and business leaders at US and UK law firms say their employees work around IT policies to get their jobs done, according to an IDG study.

Legal firms are not unique in this situation; most industries are grappling with employees who, for example, send sensitive documents from personal email accounts, or connect to the corporate server from free Wi-Fi connections in coffee shops.

These actions are not maliciously intended, yet they place the enterprise at a significant risk of compromise. Just one cyberattack or hack can cause crippling downtime, the theft of sensitive data, and damage to brand reputation.

However, rather than potentially hindering productivity with more rigid IT policies, companies should deploy systems with thoroughly integrated security to protect users, customers, and the business.

This report examines the results of a recent IDG survey into the security practices at US and UK law firms. It also offers human nature-proof strategies to protect data assets and intellectual property.

Moving in the right direction

Legal firms have put a great deal of effort into protecting their business. In the past 24 months, they have:

- Improved cybersecurity readiness (88%)
- Developed a business continuity plan (85%)
- Hired or upskilled their IT teams (81%)
- Brought in a third party to help manage threats (52%)

These steps have given them a sense of assurance: 90% say they are completely or very confident in their firm's overall security posture. Breaking that down further, they highly rate their organization's ability and sufficiency of security talent to respond to a cyberattack. In addition, 61% say they are using artificial intelligence or machine learning technologies to boost security.

Perhaps as a sign of overconfidence, 92% of legal firms say their cybersecurity posture is stronger than that of their competitors. None admitted it was weaker, and only 8% compared themselves as average against their peers.

At the same time, they are also somewhat risk-adverse: 40% of respondents cite security concerns as holding them back from deploying the latest technology and applications, with another 35% saying they're more selective with these decisions. Further, 51% say security enhancements influence their decisions to deploy new tech or apps — tied with these systems' impact on employees' productivity.

An open door to security workarounds

Despite their efforts and concerns, and an acknowledgment of emerging technology risks, law firms are facing security gaps — specifically surrounding the devices used to get work done.

For example, the majority of respondents — 82% — say their firms' employees are required to use mobile applications to do their jobs. That high percentage is not surprising given today's mobility trends, intense competition, and the long hours common in the legal industry.

BlackBerry®

CIO Custom Solutions Group

Law Firms Enable the Use of Business Tools on Personal Devices

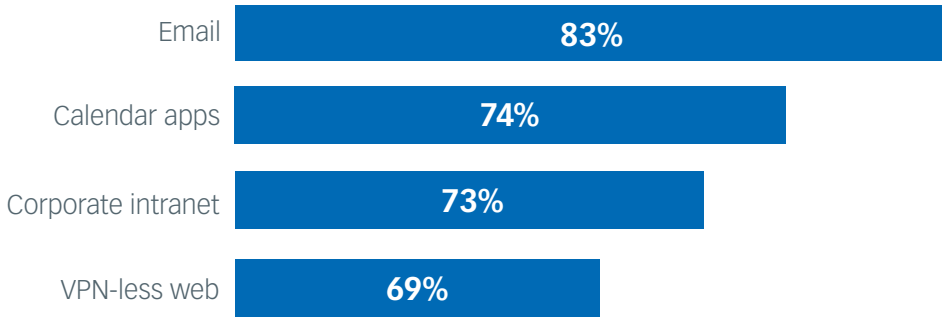

Figure 1

Source: IDG

Furthermore, most companies are open to deploying business applications across personal devices — including collaborative and communication apps that may share sensitive data such as email (see Figure 1).

The problem is that these applications are rife with risks when connections or contents are not secured. In spite of the flexibility of using mobile apps on bring-your-own-device (BYOD) devices, 79% of organizations admit that their employees still work around IT policies to get work done.

■ 30% say their employees use workarounds on a daily basis; another 43% of personnel work around IT policies more than once per week.

The use of workarounds is not malicious. It's often in the name of productivity and time savings. For example, an attorney prepping to work late night at home might email documents to a personal account, then share them from that account with external parties or clients. Or, a legal assistant struggling to send a large attachment might use a non-approved cloud storage provider to share files.

"Employees have the need and desire to get their work done and will be as creative as possible in doing so," says Nigel Thompson, VP Solutions Marketing at BlackBerry. "If the tools provided by their business are too complicated or don't allow them to complete their jobs, people will find a workaround to complete it."

The risks in workarounds

Given competitive forces and the heavy workloads of traditional law firms, it's not surprising that the need for productivity takes precedence over enforcing security.

However, the risks are great. Most of the IDG respondents say their firms suffered damage as a result of insecure file-sharing practices (see Figure 2).

Unsecured communications, apps, and devices can inadvertently open the door to malware, file-sharing hacks, and breaches. For example, without approved security policies in place, BYOD programs risk data leakage of sensitive information, including business contacts and documents.

Consider a purchase-and-sale agreement that contains sensitive, personally identifiable information. There are in-transit risks if the file is sent via an unencrypted email or cloud storage/transfer service. In addition, that document inadvertently might be stored on an unmanaged cloud provider's system without strict security controls.

Another risk is calendar apps. Security researchers recently warned that hackers are exploiting users of Google Calendar™. Event invitations might include a malicious, spear-phishing link or — worse — the invite might be faked to look like a face-to-face appointment that gives location and building access details to an intruder.

No matter whether the attack vector is email,

Law Firms Cite Damage Resulting from Insecure File Sharing

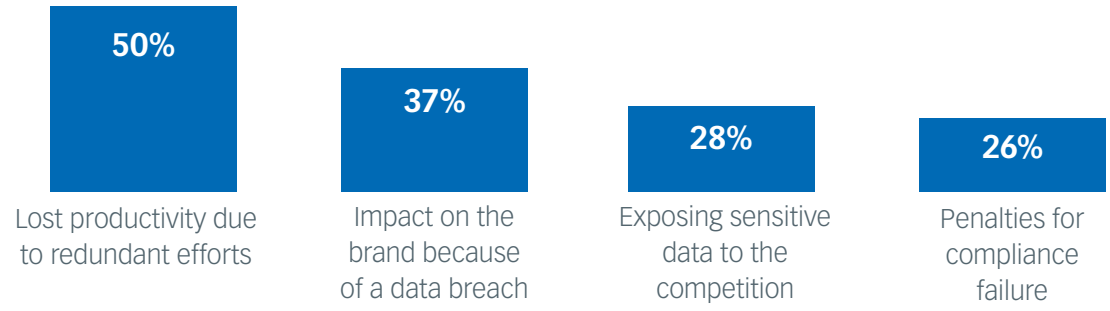

Figure 2

Source: IDG

calendar, intranets, or the web, legal firms are not immune to cybersecurity incidents:

■ Foley & Lardner, an international law firm headquartered in Milwaukee, suffered an unidentified cybersecurity breach last October. Although the organization did not disclose details, it admitted the attack "caused disruption to our IT systems," according to the firm's communication manager in an email to Bloomberg Law.

■ A ransomware attack was perpetrated on London-based DLA Piper, causing the multinational firm to shut down all computer systems temporarily. Employees were initially advised to not to use email or the company's web portal to protect sensitive data.

■ A successful spear phishing attack on O'Neill, Bragg & Staffin in Pennsylvania resulted in a shareholder sending $580,000 to hackers in Hong Kong. The firm tried to recover the funds from its bank but lost the suit.

■ Perhaps the most infamous event in recent history to affect a law firm is the Panama Papers data leak. Research uncovered a series of missteps by the international law firm Mossack Fonseca, including the transmission of unencrypted emails, a lack of network segmentation between email and web servers, as well as systems and applications that hadn't been updated for known vulnerabilities.

The risks of a breach or hack can be significant: O'Neill, Bragg & Staffin and Mossack Fonseca are no longer in business. Even without direct financial loss, a cyber incident risks damage to a company's reputation — and especially in the legal industry where trust and confidentiality are critical, that damage can be devastating.

Human-proof security

Most employees don't intentionally adopt poor security habits. However, organizations must mitigate the effects of human nature while ensuring security and privacy, especially for today's digitally-savvy users.

Here are five considerations toward intelligently protecting your firm, while enabling employees to get work done — wherever, from whatever devices they're using.

❶ Secure devices. A unified endpoint management (UEM) system can provide complete management and policy control, ensuring security for a diverse range of personal devices. UEM enables IT teams to consolidate and globally manage multiple solutions on a single platform.

❷ Secure email and applications. No matter if your firm uses customized or common business applications or a mix, it's possible to deploy a common platform to mobilize and secure all apps. The right system should offer easy integration and built-in security, as well as a seamless experience for users on both corporate and personal devices.

Market Pulse

US vs.UK Security Decision-Making

The IDG study included an equal number of respondents from US and UK law firms. Overall, organizations on both sides of the Atlantic demonstrated high levels of confidence in their security posture. However, there were a few differences in their approaches to security and technology purchasing decisions.

For example, UK firms are more likely to be using artificial intelligence and machine learning as part of their security stack: 70% compared with 50% in the US.

When considering the deployment of new technology or apps, the impact to productivity is given more consideration by US organizations, 67% of whom say it influences their decisions to a great extent, compared with 37% of their UK peers.

US firms are also more likely (67%) to cite security enhancement as a reason to deploy new industry-related technology than UK firms (37%).

❸ Secure file sharing. Users should be able to access, edit, and easily share documents and calendars from any device for a desktop-like experience. Doing so means using a service that offers full encryption and decryption according to permission rights.

❹ Secure user mobility. Enable personnel to securely work from home or a client's office with a system that seamlessly integrates commonly used apps like Microsoft® Office. For example, seek software that allows users to view, create, edit, and annotate Word docs on their personal devices while ensuring data encryption and document fidelity are preserved.

❺ Future-proof while achieving compliance and privacy. Be prepared for an expanding volume of endpoints, thanks to the growth of Internet of Things devices. By implementing a platform that secures data on any device across the mobile network and company infrastructure, the organization protects confidential data and better meets regulatory requirements.

Summary

All organizations must address the risks associated with individuals' propensity to get work done by using IT workarounds. Employee training and firewalls only go so far in an ever-evolving threat landscape.

By human nature-proofing security, law firms can reduce workarounds while improving productivity and collaboration. For example, an international law firm with offices in the UK, the Middle East, and East Asia was able to complete a large deal on a major holiday, thanks to deploying intelligent mobile security. Even though he was not in his office, the lawyer working on the deal was able to securely open the contract on his iPad, sign it, and send it back — within minutes.

"When employees can use their preferred device for work, the results include increased satisfaction, productivity, and time savings," says Nigel Thompson, VP Solutions Marketing at BlackBerry. "A cross-platform solution that supports all devices can provide employees with the flexibility they seek."

BlackBerry: Enabling Human Nature-Proof Security

BlackBerry® Unified Endpoint Management (UEM) delivers complete, unified endpoint management and policy control for the diverse and growing fleet of devices and apps in today's organizations.

With a single management platform and trusted end-to-end security, BlackBerry UEM is designed to help increase the productivity of the mobile workforce. It enables organizations to secure and manage devices, apps, data, and policies — all without sacrificing functionality or flexibility and risking user IT workarounds.

Discover how to protect your firm — and your clients. Visit: **www.BlackBerry.com/forlegal**