CONSULTING FIRMS UNDER ATTACK

HOW TO PROTECT YOU AND YOUR CLIENTS

JUNE 2018

PREVEIL

In September 2017, *The Guardian* newspaper broke the news that Deloitte, one of the world's largest management consulting firms, had suffered a major email data breach. Although largely unconfirmed by Deloitte, the breach resulted in hackers gaining access to highly sensitive information on as many as 350 of the company's clients.

Breaches like Deloitte's are incredibly damaging to client trust and can result in significant risks to future consulting work. This particular high-profile attack also serves to illustrate a larger trend: consulting firms are coming into the cross-hairs of cyber villains.

Whether you're a 30-person boutique consulting shop or 10,000+ person firm, your firm's email and digital file servers represent an extremely high value target to cyber criminals. And despite your best efforts, most experts agree it is not a question of '*if*', but rather '*when*', advanced persistent attackers will find a way into your network. To survive in this context, it's critical for consulting companies large and small to better protect the sensitive client files and emails they're entrusted with.

This white paper delves into how firms and their security teams can address this substantial business risk. The areas we will discuss include:

1. The current state of cybersecurity for consulting firms
2. Why the typical approach to security isn't working
3. Simple steps consultants can take to improve their firm's security posture

The current state of cybersecurity for consulting firms

The majority of consulting firm executives and IT teams we speak with view cybersecurity as one of the top business risks they'll face in the coming years. This certainly wasn't the case 3-5 years ago. Whether it's proprietary strategic information, valuable IP, or market-moving financial data, the end result is the same – cyber adversaries of all shapes and sizes have woken up and realized they stand to profit from relieving consulting firms of their data.

Unlike most business risks, this increasing cyber threat has the potential to produce a company-ending event. Professional services practices are fundamentally built upon client trust, and consulting firm partners regularly tell us

that any substantial loss of client data due to a cyber breach would have a devastating effect on future business.

Consulting firms typically try to hide data breaches for this exact reason. While some may succeed in the effort to keep breaches under wraps, a simple Google search highlights that Deloitte was just one of many consulting firms that have recently struggled with data security. Other high profile firms such as PwC and Booze Allen have also experienced (highly publicized) unwanted data breaches. In the case of Booze Allen, for example, classified data was inadvertently stored on publicly accessible Amazon Web Services S3 storage buckets, potentially exposing significant amounts of client data to bad actors.

Despite this threat, the IT / Security teams of many firms encounter significant pushback when they attempt to implement better security technologies and processes. Given their role as revenue generators, consultants view any changes that impact their IT environment as a negative tradeoff between an incremental security benefit and a definite disruption to consultant productivity. At the end of the day, most consulting teams are evaluated on client value delivery and billings - not how well they have executed on the firm's IT security policies. Realizing this, the security solutions most likely to succeed are those which provide a seamless user experience with minimal (if any) impact on consultant productivity.

Why the typical approach to security isn't working

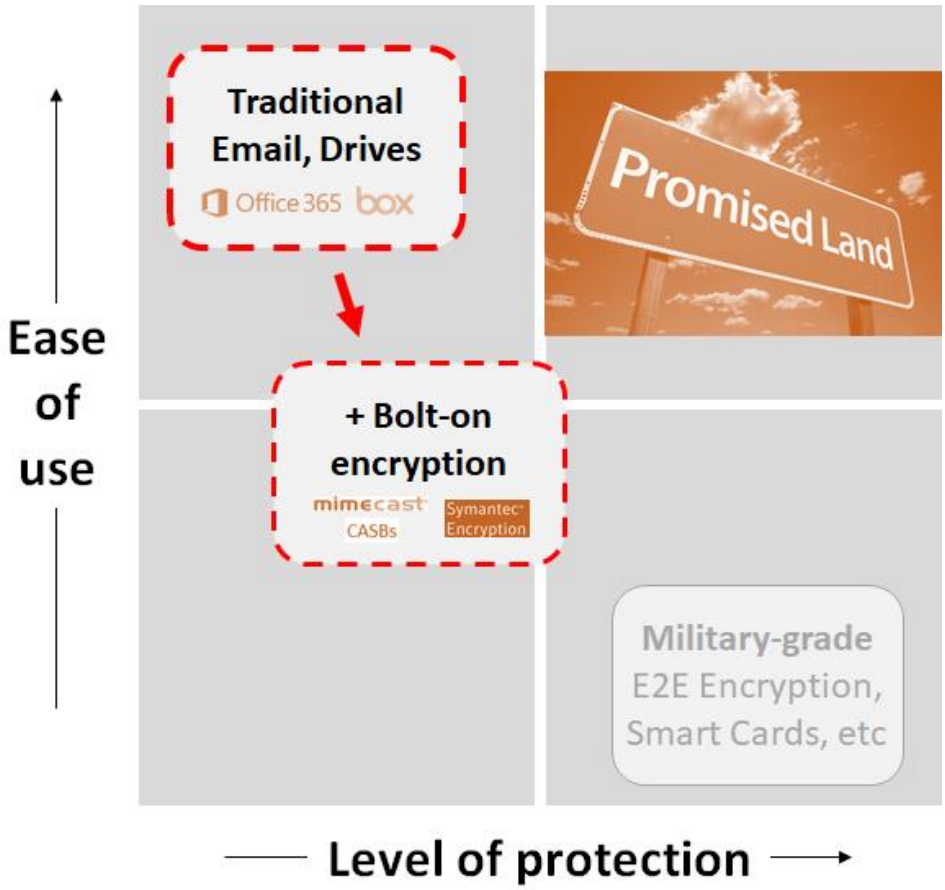
Unfortunately, the data protection strategy for many consulting firms is built upon an outdated premise of trying to keep attackers out using methods such as taller digital walls, advanced intrusion protection and alike. Yet, most cybersecurity experts agree that if advanced persistent attackers target you, eventually they will find a way in. Attackers will use methods such as stealing user passwords, compromising central points of attack like privileged admin accounts or even breaching the servers altogether.

Realizing this, the more security-conscious consulting firms have deployed a patchwork of 'bolt on' data protection solutions running on top of their existing email and file sharing systems. For example, one firm we met with recently

deployed a cloud file sharing solution + cloud access security broker solution + on-prem key safe + cloud-based identity and access management solution + Data Loss Prevention.

In taking this sort of Frankenstein approach to data security, the firm achieved a marginally better level of protection… but at an incredible cost. The end user experience was severely degraded, and a tremendous amount of IT overhead was created.

Here is a graphical illustration of the data protection paradox this firm is struggling with:



When consultants are incumbered by these 'bolt on' data protection solutions, they typically find "creative" workarounds to deliver the level of service their clients expect. For example, consultants will fall back on the time-old practice of emailing highly sensitive documents or, worse-yet, sharing them back and forth via an easy-to-use cloud storage solution like Dropbox.

End result? Despite investing significant dollars and manpower to secure their IT environment, consulting firms large and small remain vulnerable to a high probability of cyber breach.

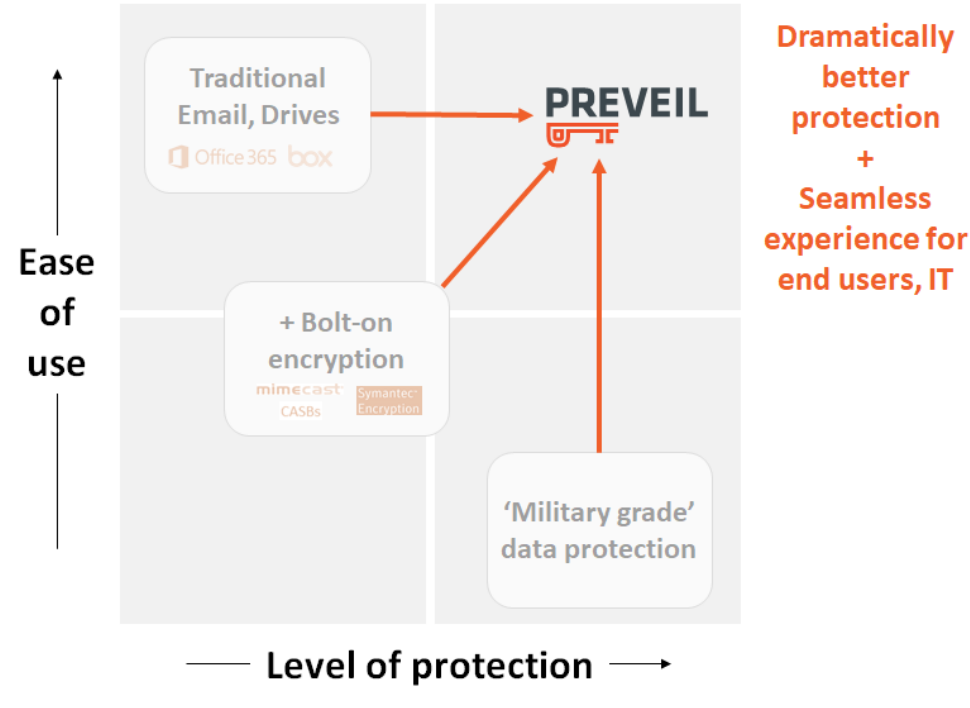
Recommendation: Simple steps to improve your firm's security posture

This paradoxical tradeoff between level of data protection vs. ease of use is at the heart of the challenge. Yet it can also be the source of a path to a better outcome.

To achieve better security outcomes, consulting firms can begin by adopting a new class of enterprise collaboration and productivity apps that are 'purpose-built' for security. At the heart of these solutions is leveraging the technology of a 'zero trust' architecture in which you assume a cyber breach is inevitable. With 'zero trust' as preamble, technologies are designed to protect data even when attacks happen by leveraging properly implemented "end-to-end encryption"

Although features vary, solutions in this new category can protect your data even when user credentials are stolen, privileged admin accounts are compromised or cloud servers are breached. PreVeil is of course one example. Wickr and Tresorit are a few others that are also gaining quiet momentum in the marketplace.

Because the security is native to these 'zero trust' apps, end-user experience isn't bogged down. IT overhead is also dramatically reduced compared to the Frankenstein situation described in the section above. Hence, as the graphic below conveys, these applications provide best-in-class data protection combined with unparalleled ease of use:



Conclusion

This white paper highlights three key themes:

(1) Consulting firms large and small have become incredibly high value targets for attackers, resulting in exponentially increased business risk for each and every firm – cybersecurity is your business whether you like it or not.

(2) Despite investing significant dollars and manpower to secure their IT environment, even security-conscious consulting firms remain vulnerable to a catastrophic data breach. This vulnerability results because of the fundamentally flawed approach of deploying a patchwork of 'bolt on' data protection solutions on top of existing email and file sharing solutions.

(3) Firms that truly want to protect their clients should consider adopting a new class of enterprise collaboration and productivity apps that were 'purpose-built' for security. With 'purpose-built apps, end-to-end encryption and distributed trust are built natively into the app itself and provide a seamless user experience consultants expect while minimizing IT overhead.

Contact sales@preveil.com to learn more

About PreVeil

Cyber-thieves are stealing massive amounts of business and personal information. Clearly, the state of the art in information security isn't good enough. At PreVeil, we aim to change that.

PreVeil is a Spark Capital-backed enterprise security company led by a team of successful technology entrepreneurs and leading cyber security experts. Inspired by MIT research, PreVeil's easy-to-use (and easy-to-deploy) end-to-end encryption solution ensures that sensitive documents and emails cannot ever be viewed by unintended recipients, even when user passwords are stolen, privileged IT Admin accounts are compromised, and servers are breached.

Learn more about how PreVeil is transforming data protection at www.preveil.com.