THE LONG VIEW

WESTLEY CHAPMAN
asks whether we can eliminate email attachments?

> "INERTIA AND HABIT SHOULD NOT BE ALLOWED TO PRECLUDE AN EVOLUTION IN COMMUNICATIONS"

Having sobered the crowd, a cyber security expert recently offered up his "one wish" to most improve data security – "eliminate email attachments". Surrounded by sceptical looks, he added "if at all possible". If potential threats would be dramatically reduced, why can't we eliminate email attachments? Inertia and habit should not be allowed to preclude an evolution in communications.

The typical network security model is medieval in its design – a fortress of high walls and vigilant sentries who scan all visitors to prevent intrusion. However, researchers perennially flag the behaviour of those protected within the walls as the single greatest security threat. And those pesky email attachments are often to blame. There are apparently a number of ways to tuck an executable bit into these attachment types. The large number of valid attachments provides cover for the very few that are malicious.

By now, we all know not to open attachments from strangers. More frequently, we never see these emails as the latest systems detect and reject them outside the wall. Yet, the cat and mouse game of identifying, exploiting and patching vulnerabilities shows no sign of ending. We are now told to accept some minimum level of malware intrusion as a given and focus resources on planning our security breach response.

The problem for most hedge fund CTOs is that employees now live in socially networked glass houses. A few minutes exploring the online presence of your firm's key employees will unearth sufficient context on at least one for a well-targeted attack. The sophistication with which an email can be made to appear to be from a trusted source and the need for defences to be 100% effective make it impossible to prevent a malware-bearing attachment from being opened inside your fortress.

As an industry, we need to embrace ongoing changes in behaviour. Many investors prefer emails with requested documents attached over self-service invitations to manager websites or ill-organised document portals. Yet document sharing services like Google Drive, Dropbox, and Microsoft SkyDrive continue to improve. The features and flexibility these services offer are already embraced by consumers as well as mid-sized businesses. If these tools lack the necessary workflow or control features to be properly integrated into institutional environments, demand them and entrepreneurs will deliver.

The paranoid will argue these tools are self-defeating by putting confidential data out into the wilderness beyond the fortress walls. For these, hardly a week goes by without more news undermining any sense of online privacy. However, some argue for a closer reading of these reports. What do open-ended subpoenas requesting voluminous data, 'back doors' supposedly built into key components, and alleged taps directly into respected private networks have in common? Encryption. More specifically, the efforts invested in these approaches lend support to the assertion that robust encryption remains secure.

Encryption will power any total shift away from email attachments to document and information sharing services. The level of encryption continues to increase with those services catering to our industry adopting the level for all stored data typically required for financial transactions and health records (256-bit AES). Some services now also encrypt user connections via the same standard used for online commerce (SSL). And now, leading services aim to encrypt data in transit between internal data centers over private networks previously thought to be secure.

Email attachments are both feared by cyber security experts and potentially outdated. Innovation reinforced with encryption will yield flexible, secure information- sharing services – eliminating email attachments sooner than we all expect. ■

WESTLEY CHAPMAN is a co-founder of AlphaPipe.com. He was previously head of ODD and risk for hedge funds at Goldman Sachs Asset Management