TrackMyRisks®

Email attachments – the looming cyber risk threatening the insurance industry

By Rachel Gordon

Supported by

BIBA

"Email becomes the weapon of choice."

Symantec

Introduction

We live in dangerous 'cyber' times for insurers, brokers and customers. As prolific senders and receivers of email attachments the insurance industry poses a high risk to itself and the customers it seeks to protect.

Cyber is one of the biggest risks (and opportunities) facing the insurance industry. Provision of insurance requires information, documentation and money, all of which are attractive ingredients for cyber criminals. Huge volumes of email attachments are sent daily; typically from insurers to brokers and then on to their clients.

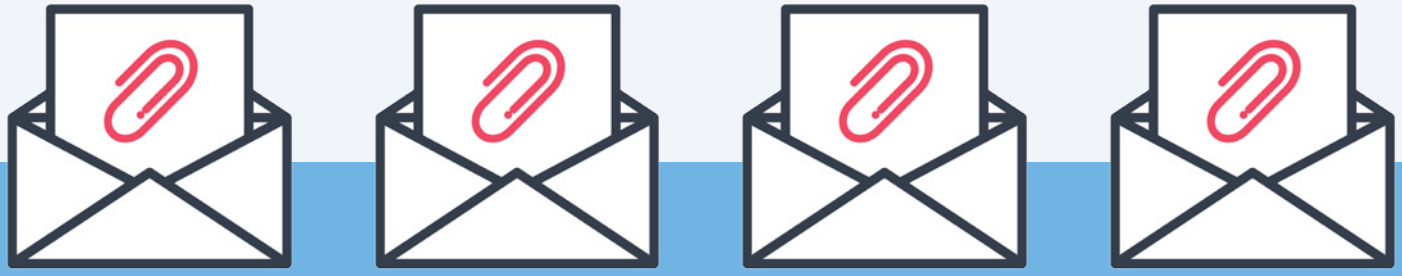
In fact, the insurance industry is culturally dependent on email attachments – while at the same time the frequency of email-borne cyber attacks are increasing. This unhealthy dependency needs to be given urgent board level attention.

Due to the scale of this cyber threat, BIBA now focuses on cyber risks in its manifesto and as a core membership issue. BIBA Chief Executive Steve White believes IT security issues must be addressed by boards and not simply handled by those with technology awareness:

"We all need to develop a better understanding of cyber risks and, for brokers, that means being able to advise on the cyber insurance market. At BIBA we want to help our members and their customers understand how the risk of cyber-security breaches can be reduced."

Managing cyber threats is a broad topic so this white paper looks specifically at the risk profile of email attachments within the insurance sector. We have also tried to use non-technical language as we believe that cyber is a whole business issue, not just an IT one.

STOP sending email attachments!



Human behaviour

Cyber crime is relatively low risk and can reap huge rewards for criminals. Malicious software – malware – is easiest to transmit via either a link or attachment and since many employees could be dealing with hundreds of emails a day, it only takes one mistake to unleash a workplace catastrophe.

So, it is no surprise cyber criminals choose email to transmit malware. Ian Grey, an information and cyber security consultant, who runs Wadiff Consulting, says: "A company's email system can make or break it. When an email system goes down, or some emails cannot be quickly delivered, productivity drops. Emails are the standard way to send text and files to anywhere on the globe and are (erroneously) trusted to be secure and auditable – unfortunately this is not the case."

Security firm Symantec's Internet Security Risk Report 2017 describes email as "the weapon of choice" and it found that 1 in 131 emails contained malware, which is the highest rate in five years. It added: "Business email scams, relying on spear-phishing, targeted over 400 businesses every day, draining $3 billion over the last three years."

Unsurprisingly, it is also a UK problem with the City of London Police's National Fraud Intelligence Bureau saying that over £32 million had been reported as lost because of email fraud.

Insurers and brokers are in a position of trust as well as being prolific senders of important documentation via email. These two factors make it far more likely that an email borne ransomware attack or fraud appearing to come from the insurer will be far more likely to succeed.

Reputation damage

One month ago, the biggest global ransomware attack took place. The WannaCry worm (initially delivered by email) spread across computer networks and with each one it reached, users were locked out of their critical data. A ransom demand of $300 in Bitcoin was then made on each infected machine.

Cyber risk modelling firm Cyence put the costs at $4 billion and even though this attack is now fading into history, one fact is certain – when one attack ends, another prepares to launch.

This attack made headlines globally. Imagine if this malicious software code had been hidden within a PDF insurance policy document!

Attractive target

One of the biggest data breaches affecting an insurer took place in the US in 2014. Anthem is one of the country's largest health insurers and a cyber breach exposed the data of some 80 million customers, including their social security numbers.

It is believed the breach stemmed from China and hackers had been operating in the insurer's system for months. A phishing email, disguised to look like an internal message, was the likely cause. Insurers are particularly attractive targets for hackers because of the detailed data they hold.

As part of their general marketing and promotion brokers may make public that they insure thousands of businesses. Whilst great from a marketing perspective these sort of facts also increase the possibility of a cyber attack in their name.

Broken processes

Manual business processes are expensive to resource from a human capital perspective but also rely on person-to-person communication, which for expediency and perceived traceability is often conducted via email.

Andrew Martin, CEO of the cyber risk scoring platform DynaRisk, comments: “Many people don’t realise that a compromised email account is an absolute gold mine for hackers. Everything is sitting in your email and it’s the means of communication with everyone you know and every online service you use.”

“If you forget your online banking password, you can just reset it via email. If you need to work on some confidential customer files over the weekend from home, you email it to yourself and if you want to get paid by a client, you email them an invoice with your account details. These are all simple and easy to do yourself, which also makes it exceptionally easy for someone else to do if they gain access to your account.”

Brokers typically handle large numbers of emails. They are the party in the middle, dealing with the insurer, customer, and other parties such as loss adjusters and of course, their own colleagues. Much of this communication is sensitive and might often be sent via insecure email. This proliferation of email attachments driven by lack of automation is exposing insurers, brokers and customers to considerable and avoidable risk.

Compliance & security

Aside from being insecure in transit, it is difficult to prove successful delivery to the recipient, the action taken by the recipient, whether they onwardly share and how they store the potentially sensitive information.

Due to the escalating threat of email, we expect tighter controls over inbound emails with attachments to become commonplace. In the immediate aftermath of the WannaCry attack, it was reported that Aviva closed their systems to inbound emails with attachments for 4 days.

With the increasing threat posed to organisations by inbound email attachments and the tightening regulatory regime in the insurance sector, serious thought is needed right now about replacing email attachments as the primary means of communication.

Stop sending - start sharing

If your firm is overly dependent on email attachments for customer communication, then make a management commitment to stop it, or at least reduce it over time.

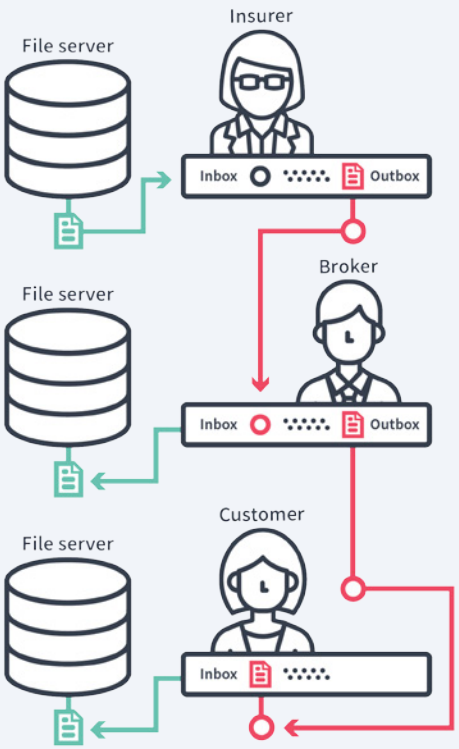
For example HMRC clearly states to all taxpayers:

"HMRC will still never email you about rebates or to ask for your bank account details and these emails won't contain any confidential information."

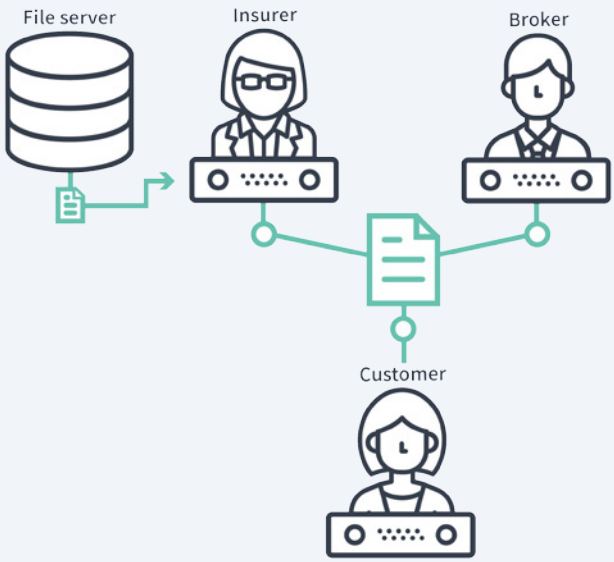
Taxpayers are conditioned to be suspicious of sensitive emails that appear to be from HMRC as opposed to being trusting. Perhaps the insurance industry or individual firms could make a similar pledge?

Email attachments are not the only means of transmitting documents (usually PDFs) from one person to another. The simplest way to stop sending is to share the documents in a secure online environment, which can be securely accessed by the insurer, broker and client.

Stop sending



Start sharing



There are a wide range of document sharing systems on the market at a range of price points including:

Summary

Email attachments are risky, inefficient and insecure. Removing them from the insurance process will take time but it is our belief that the work should start now.

DynaRisk's Martin comments:

"The insurance industry needs to move away from email as a primary means of communication. Many companies are running transformation programs to reduce their reliance on these legacy communication methods in favour of secure collaboration and sharing. By moving towards these technologies, companies can greatly reduce cyber risks related to email, improve the efficiency of their workforce and the experience of their customers."

Glossary of most common cyber risks associated with email attachments

Ransomware

Computer code that prevents or limits users from accessing their data, either by locking the screen or files, until a ransom is paid.

Spear phishing

Email that appears to come from a trusted source that seeks to trick the recipient into taking an action such as transferring money, paying an invoice or divulging passwords.

Viruses

Computer code that infects the user's machine and potentially then spreads to others.

TrackMyRisks®

TrackMyRisks - is an insurance-friendly, SaaS document management system that powers secure and auditable file sharing between insurers, brokers and clients.

www.TrackMyRisks.com

BIBA

The British Insurance Brokers' Association (BIBA) is the UK's leading general insurance intermediary organisation representing the interests of insurance brokers, intermediaries and their customers.

www.biba.org.uk

Follow us on Twitter
@TrackMyRisks