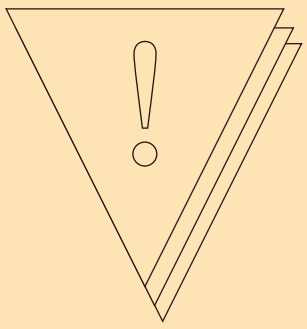
The risks of using PDF

Today, annual reports are increasingly being published both in a print format and through the company's website. Usually, reports can be downloaded as pdf – this way, the version that is available online looks the same on a desktop screen as in the print version. In the creation process, it is easy to convert, and being delivered, the reader cannot make any changes. Seems perfect. However, is pdf really the digital solution companies should choose?

By Arron Finnon



From a cyber-security perspective, the Portable Document Format (PDF) has had a very jaded past. Over the years numerous security vulnerabilities have been discovered in PDF viewer software, which has only been overshadowed by the sheer amount of cyber attacks that could be launched from within the PDFs themselves. Few document formats can boast such a history of falling foul of hackers quite like PDFs, except maybe the Excel spreadsheets format and its history of macro abuses. All of this paints a worrying picture and of course this is only heightened by PDF's growth as a "go-to" document format for large numbers of businesses using it for external communication. PDF's route to success can almost be seen as an ironic homage to economy's very real need of a cross-platform document format that can be relied upon to deliver documents to users, customers, and investors alike. However, those environment conditions of the past which pushed PDF as a solution do not really exist anymore. Modern day consumption of information is a far bigger issue than readability: it is about customizing surfaces, responding, searching, generating data as well as corresponding securely, generating a new interactive public in the World Wide Web. We are using out smart phones more than desktops – we need to understand complex information, facts and figures looking at them in a very short amount of time and on a limited space on our devices. We cannot afford static formats any longer for these claims we have to modern information transfer.

PDF seems to be a go-to request

Along with the many security issues that PDFs have brought to businesses front-doors, it is also quite limited as a medium to deliver information. There is no real way to know what type of device a person is going to view your PDF on until they've downloaded it. Just because something looks nice, clean and easy to read on a laptop screen doesn't mean your reader isn't going to be struggling to view that important graph on his smartphone screen. People comment that the reason they produce PDFs is that it is what their readers want. This may very well be true, but what is really happening is readers just want something to read without too much hassle or fuss. No one specifically asks for a document in PDF format because the reader is a big fan of the product. PDF seems to be the go-to request when the user struggles to open a word-type document.

As someone who is paid to think of what black-hat hackers can do to businesses, the use of PDFs is something that I just can't get behind. The rule-of-thumb in most security compromises is that if a hacker is not detected within the first few minutes then it is going to be anywhere upwards of 24 months before it is. That can allow for at least two annual reports that could be potentially weaponised and used to deliver further cyber attacks on a business or its investors. This may seem like a Hollywood movie plot, but this is what happens in real life: Earlier in 2017 the airline industry was targeted in a campaign were PDFs were used to infect victims with malware once they were opened. Once a victim has been infected with malware, an attacker can steal, encrypt or delete sensitive data, monitoring a victim's internet traffic, access the camera and microphone of a victim's device without them knowing, and install further malicious software. In the end the victim's device is completely compromised and everything it does is under the control of someone else. In May of 2017 the ransomware known as "Locky" also infected victims using PDFs. Ransomware takes a victim's data and encrypts it making it totally inaccessible to its owner. Only when the ransom is paid, the victim's files get unlocked. It's worth noting that paying the ransom is by no means a guarantee that files will be decrypted. Many companies have faced major damages through so-called cyber-crime. Some big corporations had to shut down their business completely, such as HBGary. Not seldom, CEOs had to take responsibility for negligence and had to resign for severe damage of virtual company assets, just like Marissa Mayer of Yahoo. Of course: the cause for such business dramas have not always been PDFs. But PDFs seem to be one of the major vulnerabilities in financial markets communications and interactions.

Would you question to open a PDF?

Many readers of this article wouldn't question opening a PDF in their e-mail, especially if the sender looks vaguely familiar. Yet I guess that none of the readers would question opening a PDF they just downloaded from a company's website, wanting to read its annual report. One really needs to question why a business would accept additional risks, especially when the file format doesn't really offer any additional benefit.

The only real answer has always been the use of open-document formats, or at the very least a format that allows documents to be rendered in HTML; in non-geek speak: allowing your documents to be viewed natively in Web browser. It is now trivial for most Web pages to be responsive to the device viewing it. It may also give far better metrics of how readers are consuming the report as well. When needed, there can also be off-line versions to be made available too. We will never be short of people that can write good quality code that can be viewed in a Web browser, and nearly all internet-facing devices can read reports without the need of installing any additional software. In the end, the Web is one of the first real cross-platform product waiting to be used appropriately.

ARRON "FINUX" FINNON
has been involved in security research and consultation for over twelve years. His security research and consultation have helped businesses around the globe to develop the effectiveness of their security posture in detecting and mitigating cyber attacks.