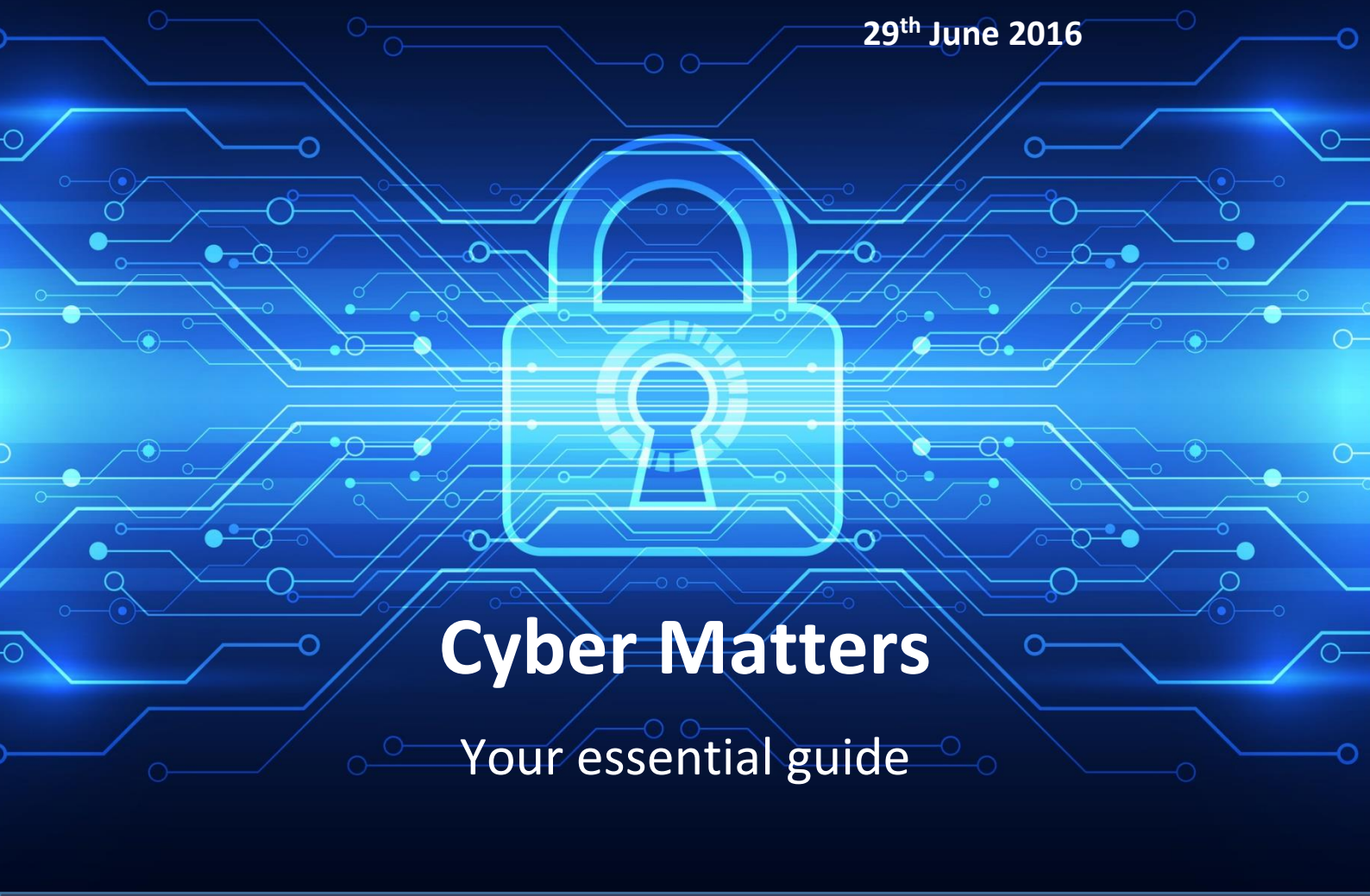
29th June 2016



# Cyber Matters

## Your essential guide

### In this issue




01704 542 420
info@p-ccomms.com

# Cyber Matters - BREXIT ISSUE

**BREXIT: What next for Cyber?**
The impact of Britain's exit from the EU remains unknown, but this hasn't stopped the cyber community speculating as to what the ramifications may be for cybersecurity, privacy and cybercrime-related activities. Here are the top 3:

1. **UK digital strategy put on hold**

The UK government's long-awaited digital strategy is likely to be put on hold. The strategy was intended to comprise policy from a number of departments to outline plans for the UK's digital infrastructure. Brexit will pose a huge technocratic challenge for Whitehall as the UK seeks to untangle EU policy and regulations.

2. **Full compliance with GDPR**

New General Data Protection Regulation, which comes into force in May 2018, will impose very precise, non-negotiable requirements for handling EU residents' personal data, and any organisation that does business in the EU must demonstrate that they are handling such data in a safe manner. The UK Parliament could opt to not fully comply with the GDPR, but there is a strong business case for them to do so.

3. **Cybercrime-related challenges**

Brexit is likely to lead to a significant reduction on cooperation in criminal and policing matters between the UK and the EU. For example, the UK works with the EU law enforcement intelligence agency Europol which is led by British civil servant Rob Wainwright and its "EC3" European Cybercrime Centre is led by fellow Brit Steven Wilson. The UK would probably lose full access to EU agencies, and could only participate as an associate.

# You've Got Mail

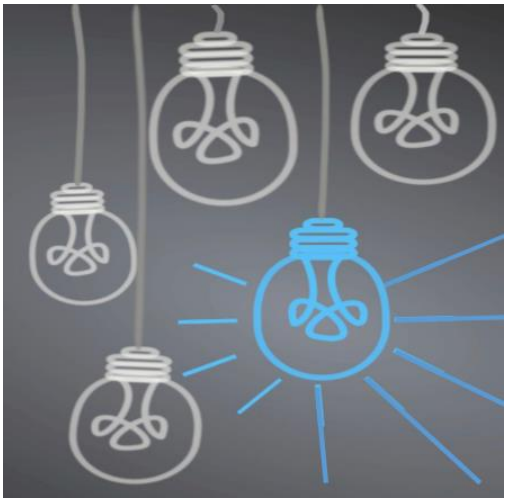
An Austrian aeronautical company, Fischer Advanced Composite Components AG (FACC), has been targeted by cybercriminals who used a business email compromise (BEC) scheme to net £32 million through a spear-phishing attack.

FACC is a major designer and manufacturer of aircraft components and systems, with a client base that includes Boeing, Airbus, Rolls-Royce, Siemens SAS and Mitsubishi Heavy Industries. Reporting suggests the incident occurred last January and involved a fake email that impersonated the then CEO Walter Stephan, requesting one of FACC's financial department employees transfer 50 million Euros that was supposedly for one of the company's acquisition projects.

FACC, realizing that they had been scammed, adopted countermeasures and were able to stop the transfer of 10.9 million Euros on the recipient accounts. The rest of the money, however, is believed to have already disappeared in Slovakia and Asia.

**Please see over page for a fuller explanation.**

# Business Email Compromise



Quite simply, official business email accounts are compromised to conduct unauthorised fund transfers. BEC scams often begin with an attacker compromising a business executive's email account. This is usually done using keylogger malware or phishing methods, where attackers create a domain that's similar to the company they're targeting, or a spoofed email that tricks the target into providing account details.
Upon monitoring the compromised email account, the fraudster will try to determine who initiates transfers and who requests them. The perpetrators often perform a fair amount of research, looking for a company that has had a change in leadership in the finance function, or companies where executives are travelling. BEC scams have three versions:

**"The Bogus Invoice Scheme"**
Usually involves a business that has an established relationship with a supplier. The fraudster asks to transfer funds for invoice payment to an alternate, fraudulent account via spoofed email, telephone, or fax.

**"CEO Fraud"**
Fraudsters identify themselves as high-level executives purporting to be handling confidential or time-sensitive matters and initiate a transfer to an account they control. This scam is also known as "Business Executive Scam", "Masquerading", and "Financial Industry Wire Frauds".

**"Employee Hack"**
An email account of an employee is hacked and then used to make requests for invoice payments to fraudster controlled bank accounts. Messages are sent to multiple vendors identified from the employee's contact list. The business may not become aware of the scheme until their vendors follow up to check for the status of the invoice payment.

Checks on how to be careful:

- Carefully scrutinize all emails.
- Review emails that request transfer of funds
- Educate and train employees
- Verify any changes in vendor payment location by using a secondary sign-off
- Stay apprised of customer habits including the details, and reasons behind payments
- Confirm requests for transfer of funds when using phone verification as part of two-factor authentication, use known familiar numbers, not the details provided in the email

Thank you for downloading this guide.

Please feel free to contact us on the details below if you have any questions or comments, or would like advice on any of your own cyber security issues.

**01704 542 420**
**info@p-ccomms.com**