FOR IMMEDIATE RELEASE

AIG Contact: **Hannah Scott**, External Communications Manager, AIG Europe Ltd
hannah.scott@aig.com +44 20 7954 7289
EEF Contact: **Hilary Douglas** +44 7867 179 163

PRESS RELEASE
AIG
The AIG Building
58 Fenchurch Street
London
EC3M 4AB
www.aig.com

Industry urged to boost cyber defence investment as almost 50 per cent of manufacturers report attack – EEF/AIG survey

Nearly half of manufacturers have been the victim of cyber-crime, and a quarter have suffered some financial loss or disruption to business as a result, according to a new report published today.

The manufacturing sector is the third most targeted for attack, with only government systems and finance more vulnerable. Yet manufacturing - which has 2.6 million employees, provides 10 per cent of UK output and 70 per cent of business research and development - is amongst the least protected sector against cyber-crime in Britain.

The new report, Cyber-Security for Manufacturing, published by EEF, The manufacturers' organisation and AIG and carried out by The Royal United Services Institute (RUSI), pinpointed the susceptibility of manufacturers to cyber risk, revealing that 41 per cent of companies do not believe they have access to enough information to even assess their true cyber risk. And 45 per cent do not feel that they do not have access to the right tools for the job.

Cyber threat is holding back companies from investing in digital technologies, with a third of those surveyed nervous of digital improvement. Moreover, a worryingly large 12 per cent of manufacturers admit they have no technical or managerial processes in place to even to start assessing the real risk.

One of the easiest forms of cyber-attack comes through poorly protected office systems, often the first implemented historically within manufacturing businesses. The report looks at a number of real-life examples, including two where companies production systems were infiltrated and severely disrupted after hackers gained access to their IT systems by initially hacking into unprotected office software, used to keep HR and admin records.

Commenting Stephen Phipson, CEO of EEF, The manufacturers' organisation said:

"More and more companies are at risk of attack and manufacturers urgently need to take steps to protect themselves against this burgeoning threat.

"EEF has a vital role supporting manufacturers in the face of this challenge and we are working closely with RUSI, whose world-leading Cyber Security Research Programme is well established as a key voice to understand the fight against the threat of ever evolving cyber-crime to the modern business..

"We know businesses cannot afford to ignore this issue any longer and while we welcome government's progress in improving cyber-security resilience, to date through the work of the NCA and NCSC, there needs to be an increasing focus given to the specific needs of manufacturing, which hitherto has been lacking.

"Failing to get this right could cost the UK economy billions of pounds, put thousands of jobs at risk and delay the supply of essential equipment to key public services and major national infrastructure projects. I hope this report underlines the critical risk to government and industry".

Romaney O'Malley, Head of UK Regions & Head of Industrials at AIG Europe added:

"For many manufacturers, cyber risk is still not considered a principal risk on the risk register. Nevertheless, the cyber threat landscape has evolved over the last year, with attacks becoming more sophisticated and more broadly disruptive. There is an increasing level of state-sponsored attacks between nation states, where companies infected by malware may just be collateral damage. The potential threat from cyber-crime is widespread.

"There is evidentially significant need for greater awareness and understanding of the importance of cyber risk management, not only to protect existing businesses, but to create more secure environments to grow and capitalise on the potential that digital technology advances bring to manufacturers."

Dr Karin Von Hippel, Director General of RUSI said:

"The importance of the manufacturing sector to the security of the UK economy cannot be overstated. Increasing digitisation creates further opportunities, but also exposes us to potential vulnerabilities to cyber-attacks, whether from criminals or nation-state adversaries. The sector needs to recognise these risks and respond accordingly."

The report urges companies to begin a programme of continuous assessment of which people, information and technologies are critical to their organisation and undertake real-time scenario planning to map out the consequences of a cyber-security infrastructure or data breach. More and more customers are demanding cyber security

guarantees from their suppliers and over a third of manufacturers admitted they could not to this.

There are five technical controls in Cyber Essentials:

1. Use a firewall to secure your Internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware by using antivirus software, only downloading apps manufacturer-approved stores, or running apps and programs in an isolated environment
5. Keep your devices and software up to date by patching regularly.

ENDS

Notes to editors:

Full report:
https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cyber-security-for-manufacturers

Case studies

GERMAN STEEL MILL MELTDOWN
While the exact details of the company involved are still unknown, the attacker used sophisticated social engineering and spear-phishing tactics to hack into the steel mill's office computer network. Crucial controls were tampered with, making it impossible to turn off the blast furnace. The result - massive damage to the foundry.
The attacker, likely an industry insider or someone working with an insider, had specific knowledge of the production processes involved so that maximum damage could be done to the normal workings of the mill. The company's systems were specifically vulnerable because the office network was connected to the industrial control system, meaning the attackers could effectively take control of production – and stop it from happening.

INDUSTRIAL CONTROL SYSTEM ATTACK IN SAUDI ARABIA
In August 2017, a petrochemical manufacturer in Saudi Arabia was infected with malware that investigators believe was not simply designed to steal data or shut down operations but potentially to cause a catastrophic explosion. Significantly, it targeted operational technology in the form of industrial control systems rather than the more traditional focus on information technology.

Whilst the identity of the company affected and the likely attackers remain unclear, it has been revealed that the target was part of the facility's safety system, designed to stop automated equipment going beyond safe operating conditions. The malware was designed to override this.
The attack was not intercepted by the cyber security measures in place and failed only because as the developers of the malware had made an error in the code that caused the systems to simply shut down safely. It is likely that the perpetrators will have since fixed this error.

The EEF Cyber-security survey was conducted in February 2018 and is based on a sample size of 161 responses from individual UK-based manufacturing businesses, 98 of whom were Small and Medium-Sized Enterprises (SMEs) as per the UK-government definition

About EEF

EEF, the manufacturers' organisation, is the representative voice of UK manufacturing, with offices in London, Brussels, every English region and Wales. This year we celebrate 120 years of backing Britain's makers.
Collectively we represent 20,000 companies of all sizes, from start-ups to multinationals, across engineering, manufacturing, technology and the wider industrial sector.
We directly represent over 5,000 businesses who are members of EEF. Everything we do – from providing essential business support and training to championing manufacturing industry in the UK and the EU – is designed to help British manufacturers compete, innovate and grow.
From HR and employment law, health and safety to environmental and productivity improvement, our advice, expertise and influence enables businesses to remain safe, compliant and future-focused.

More information at www.eef.org.uk

About AIG

American International Group, Inc. (AIG) is a leading global insurance organisation. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release.