

CYBER DECODER

FINANCIAL LINES GROUP NEWSLETTER ISSUE 14



DATA PROTECTION CLAIMS

Page 3

PCI COVER: EXPECTATION VERSUS REALITY

Page 4

IT STARTED WITH A TWEET

Page 5

ALSO IN THIS ISSUE

Cyber risks dominate finance	3
Privacy Impact Assessments	6
Cyber threat intelligence	7
Top Tweets	8

Making the best of it: time to address cyber risks in manufacturing

Cyber security is among the biggest business risks identified by US manufacturers, and IBM says the sector is the most commonly targeted by attackers after healthcare. Yet British manufacturers are not taking the dangers seriously.

A survey by the EEF, “the voice of UK manufacturing and engineering,” published in May shows a worrying failure to address these risks: 46% overall, and over half of small manufacturers, haven’t increased investment in cyber security in the past two years; only 56% say their board gives cyber security serious attention; one in five don’t make employees aware of cyber risks; and little more than a third have an incident plan in place.

“Our survey highlights that investment in new technology isn’t being matched by investment in managing risks, especially among smaller firms,” said the EEF’s Chief Economist Lee Hopley.

A PRIME TARGET

Part of the worry is that this leaves businesses with inadequate defences against targeted attacks. IBM’s 2016 [Cyber Security Intelligence Index](#), shows manufacturing ahead of even financial

services based on the number of cyber attacks and incidents worldwide last year. A lack of headline-grabbing, large-scale attacks is offset by the frequency with which manufacturers were targeted. The automotive industry (accounting for 30% of attacks) and the chemicals industries were most at risk, it found.

These findings are supported by other reports. The US Department of Homeland Security, for instance, [says](#)

Continued on page 2 ►►



investigations of cyber attacks on the nation's critical manufacturing sector nearly doubled last year. Cyber risks have also entered into the top ten risks in big manufactures' disclosures to US regulator the Securities Exchange Commission, according to accounting firm [BDO](#).

"While the industry may have flown under the radar as high-profile attacks against the retail, financial services and healthcare industries made headlines, manufacturers' information, intellectual property and products have become prime targets for cyber criminals," [its report](#) notes.

Of course, there have been high profile cases and concerns – whether over [hacking cars](#) (a real risk, [says the FBI](#)) or the potential for [physical damage from cyber attacks](#) on heavy industry.

Most attacks, though, notes IBM's report, are simply looking to steal money or intellectual property. A bigger danger for many, however, may be more prosaic still: simple technology failure.

Behind the challenges facing manufacturing, say [EEF](#), is the fact that the sector is in the midst of a [fourth industrial revolution](#). It is based on increased automation, data exchange, wider supply chain communications, and technology such as the Internet of Things. It is also one that many manufacturers [do not fully understand](#).

[Behind the challenges facing manufacturing, say EEF, is the fact that the sector is in the midst of a fourth industrial revolution.](#)

These changes don't just increase the risk of cyber attacks on manufacturers; implementation and integration of new systems, opening new communication and control paths, training staff and changing work patterns all increase the risk of errors and technology failures resulting in business interruption.

For manufacturers this can be among the most valuable aspects of cyber insurance policies, which can respond to business interruption (BI) caused by technology failure, even if there is no cyber attack. The waiting periods before the policies pay can be as low as eight to 10 hours, compared to 48 hours to a week under the limited extension available for 'non-damage' BI in the property insurance market.

Industry 4.0 is bringing a whole range of new cyber and technology risks for manufacturers, and by and large, the insurance market is ready to respond. ■