Cyber Security: A Moving Target

SMMT Automotive Quality Management Systems Conference

2019

Claire Russell, Director, NQC Ltd

NQC

Agenda

- Key trends that impact on cyber security
- The automotive industry response to manage cyber risk
- The launch of the AIAG Cyber Initiative

NQC

The continued move towards globalization

- Growth of global players through mergers and acquisition
- Desire to be bigger and focus on economies of scale
- Specific examples within the automotive sector

NQC

The changing dynamics of the supply chain

- Impact of globalization
  - Compressed/flatter supply chains
  - Includes direct engagement with sub-tiers
  - Global in nature
- Change in product focus e.g. electric
  - New technologies and ways of working emerging
  - Collaboration for innovation – flow of ideas between supply eco-system
  - Innovation partners not fillers of purchase orders

NQC

Digital by default creates additional challenges

- Exponential digital growth
  - Data volumes will be 50 times greater in 2020 than in 2016 – Microsoft
  - Cloud data center traffic will represent 95% of all data center traffic by 2021 – Cisco
  - “Big Data Bang” - IoT world from 2 billion objects in 2006 to 200 billion objects in 2020 – Intel
- Location, Location, Location
  - Wysteria Lane vs Cyberville

NQC

More than half of British firms 'report cyber-attacks in 2019'

Hackers went undetected in Citrix's internal network for six months

60 Percent Of Small Companies Close Within 6 Months Of Being Hacked

SURVEY FINDS CYBER ATTACKS INCREDIBLY COMMON AT AUTOMOTIVE FIRMS

Businesses are overlooking the threat of cyber attacks to their supply chain that may cause significant lost income and increased operating expenses.

That's the warning from insurance broker and risk management firm *Marsh*. It explained such threats have affected more than half (52 per cent) of co responding to the Business Continuity Institute's *Supply Chain Resilien* report.

Small business owners shouldn't assume they have nothing worth hacking

Small doesn't mean safe: why SMEs are a target for fraudsters

UK small businesses targeted with 65,000 attempted cyber attacks per day

Cyber Crime– Attack vectors are varied

30% of phishing emails in the US are opened Verizon 2018 Data Breach Investigations Report	• Cyber crime isn't just about technical controls/protection • User education is just as important – can't underestimate the human element • Phishing emails lead to viruses, sharing of sensitive personal information etc.
Over 24,000 malicious mobile apps blocked daily Symantec Internet Security Threat Report	• Applications can contain malware that can infect a network • Uncontrolled corporate environments allow users to download apps and potentially let hackers in • The blurred line when staff use personal devices at work leads to greater risk
Major ISP sees 80 billion malicious scans a day McAfee Economic Impact of Cyber Crime 2018	• Cyber criminals are constantly searching for an unlocked door to enter • Unconfigured equipment (servers, firewalls) can make it easy for cyber intruders • Once in, cyber intruders can keep coming back for more

Cyber Crime – have you already been a victim?

43% of businesses were a victim of a cyber security breach in the **last 12 months**

UK Government - Cyber Security Breaches Report 2018

A business becomes a victim of a ransomware attack every **14 seconds**

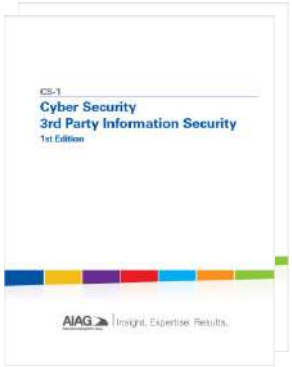
Cybersecurity Ventures - 2018 Data Breach Investigations Report

61% of cyber breach victims are businesses with **under 1000 employees**

Verizon - 2018 Data Breach Investigations Report

Addressing cyber security as an industry – recap on progress to date

- OEMs and AIAG came together to collaborate on a common set of cyber requirements
- Contributors included information security specialists and supply chain risk management leads
- Led to the creation of Automotive Industry 3rd Party Information Security Requirements – published in 2018
- Partnership with NQC to support the roll-out at scale



Launching the AIAG Cyber Initiative

- Creation of two complementary products to help suppliers understand the Information Security Requirements and how they compare to them
  - **Cyber Risk Assessment** – Basic and Advanced options to suit a supplier's capability level
  - **Cyber Virtual Audit** – remote vulnerability scan with varying cadence to provide assurance
- Accessed by invitation from an OEM or via the AIAG Member Cyber Initiative
- Communications on how to access will be shared over the coming weeks (some OEMs have already started)

NQC