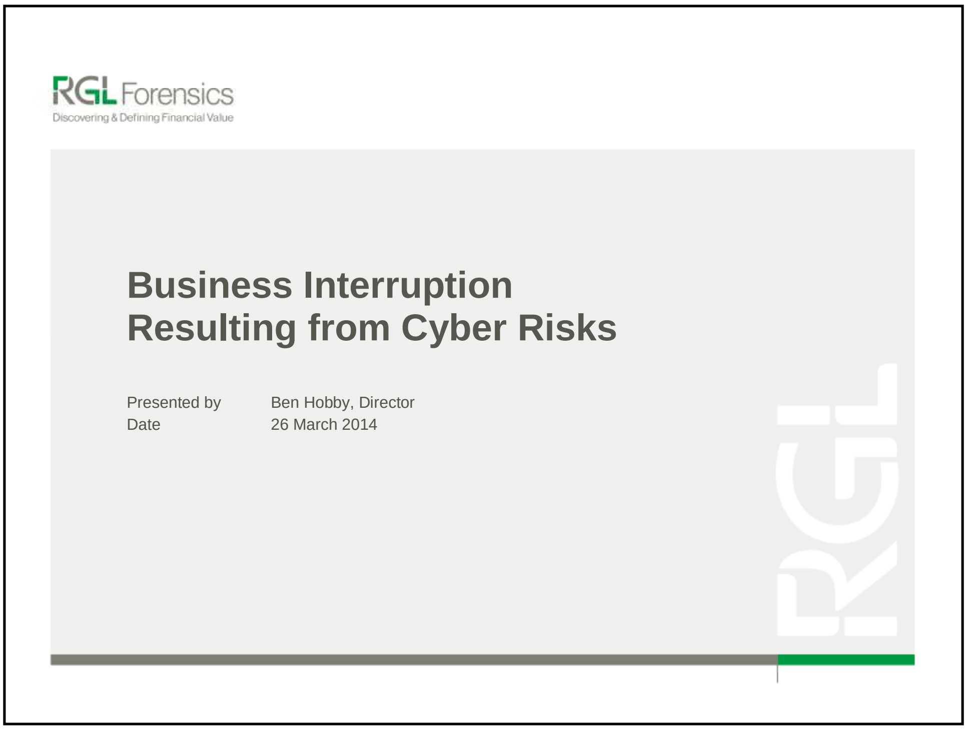
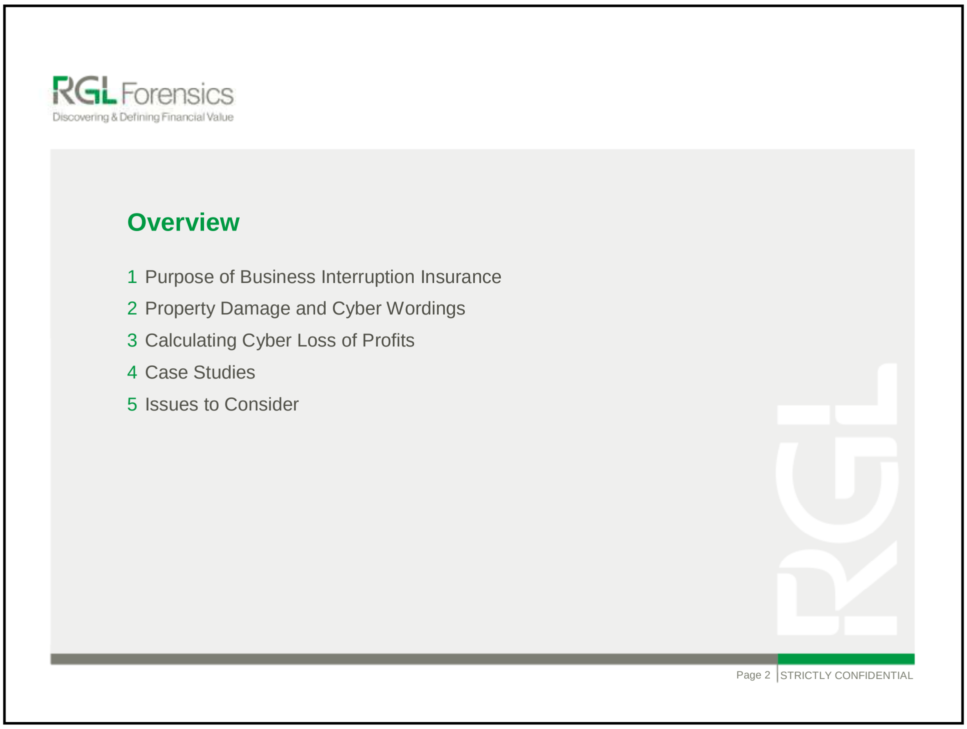


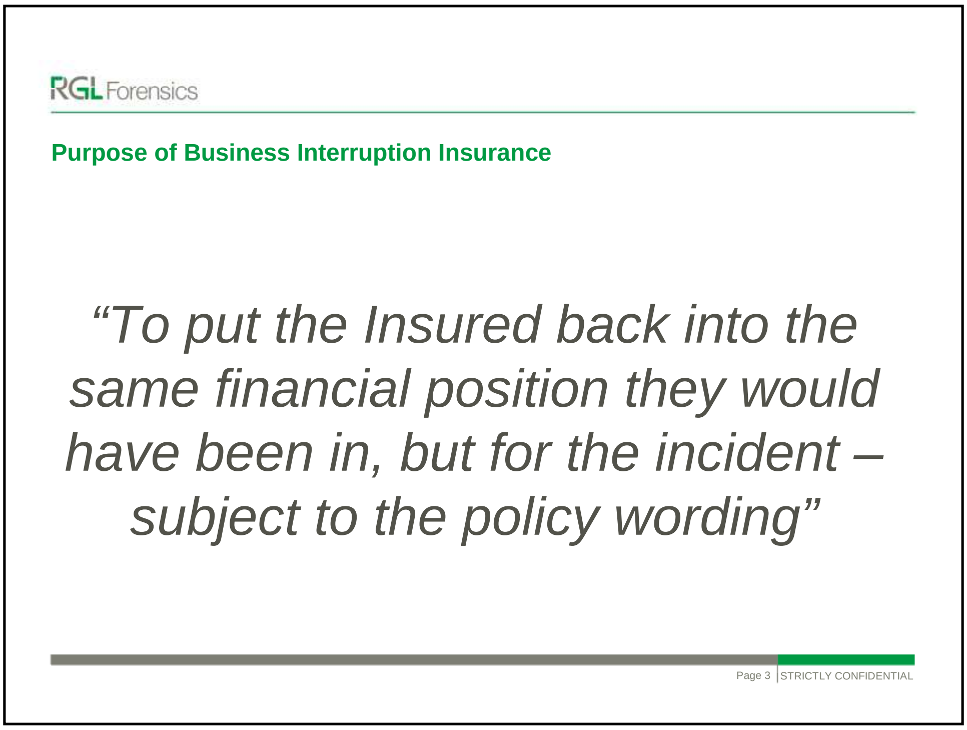
Business Interruption Resulting from Cyber Risks

Presented by	Ben Hobby, Director
Date	26 March 2014



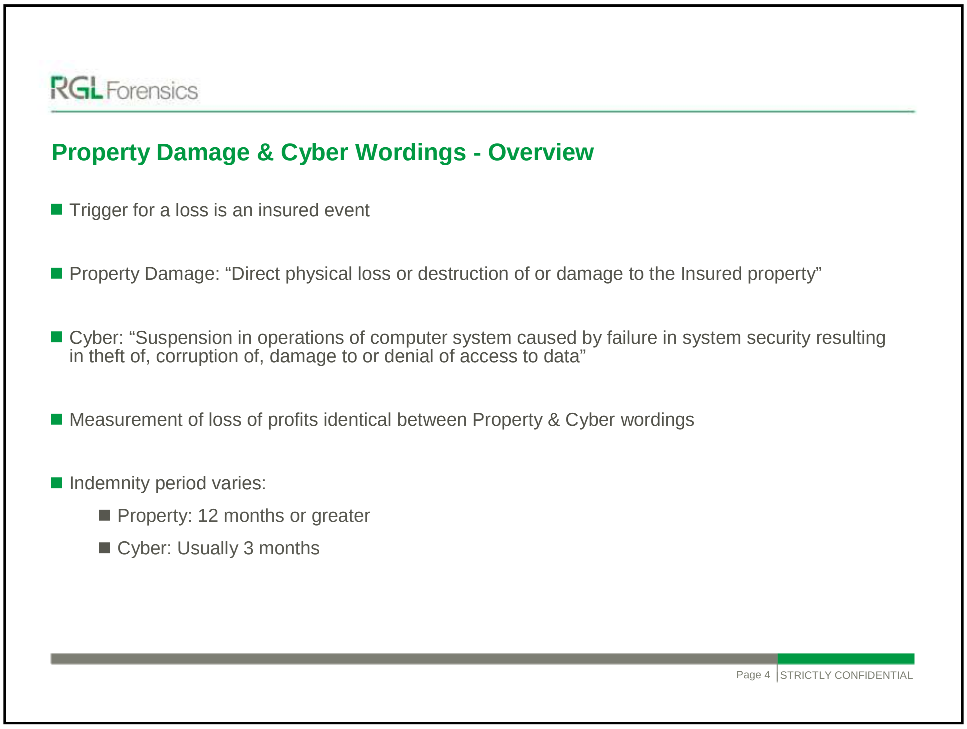
Overview

1 Purpose of Business Interruption Insurance
2 Property Damage and Cyber Wordings
3 Calculating Cyber Loss of Profits
4 Case Studies
5 Issues to Consider



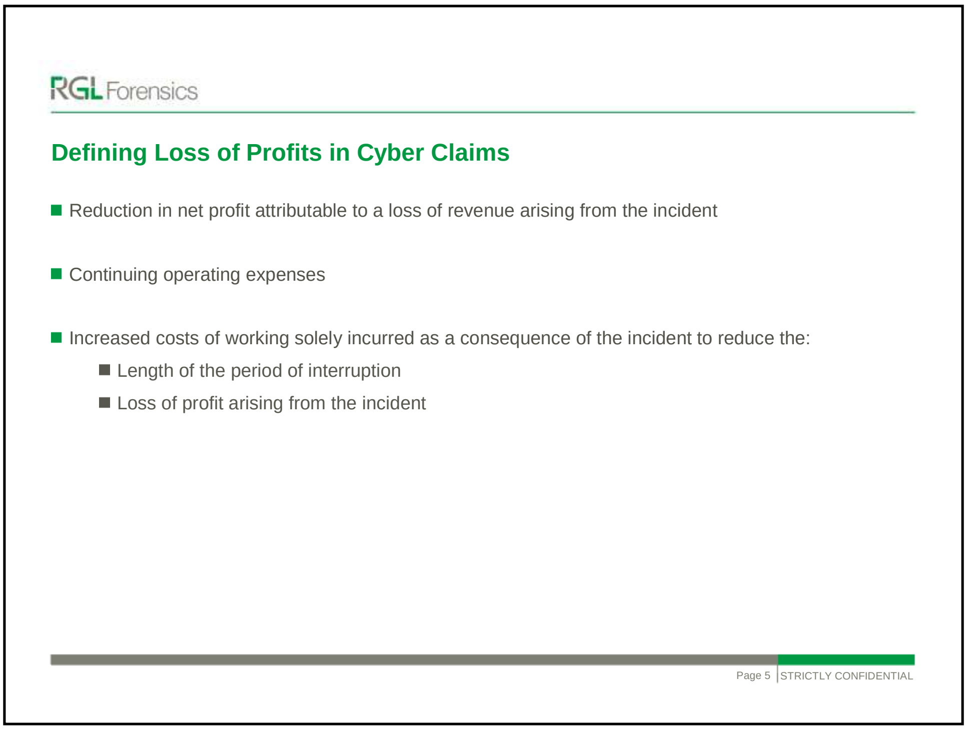
Purpose of Business Interruption Insurance

“To put the Insured back into the same financial position they would have been in, but for the incident – subject to the policy wording”



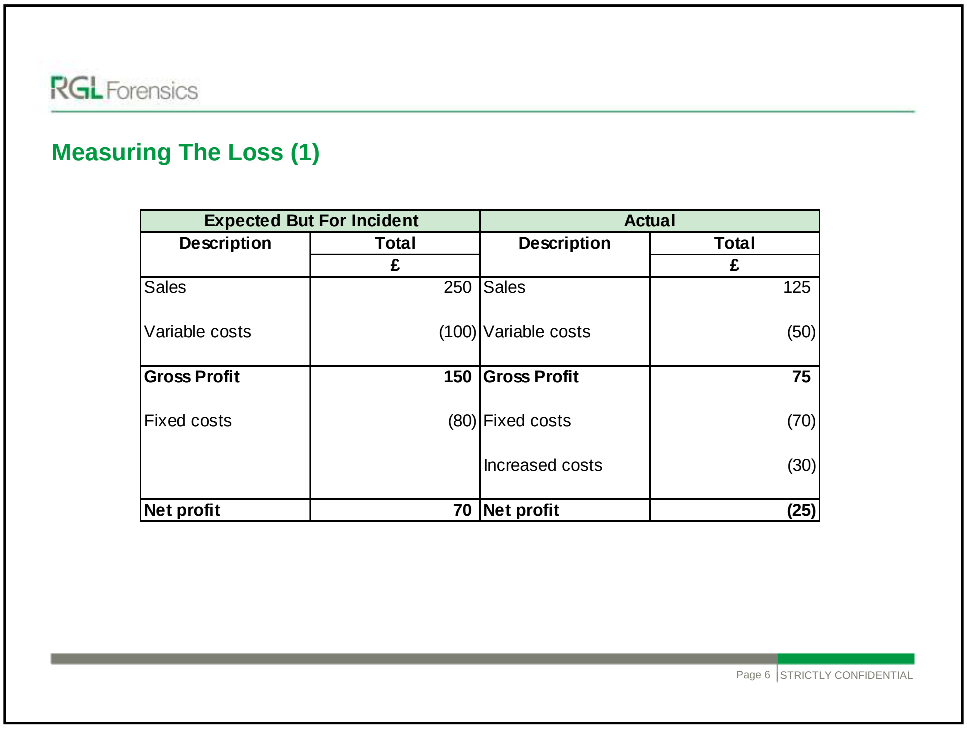
Property Damage & Cyber Wordings - Overview

- Trigger for a loss is an insured event
- Property Damage: “Direct physical loss or destruction of or damage to the Insured property”
- Cyber: “Suspension in operations of computer system caused by failure in system security resulting in theft of, corruption of, damage to or denial of access to data”
- Measurement of loss of profits identical between Property & Cyber wordings
- Indemnity period varies:
  - Property: 12 months or greater
  - Cyber: Usually 3 months



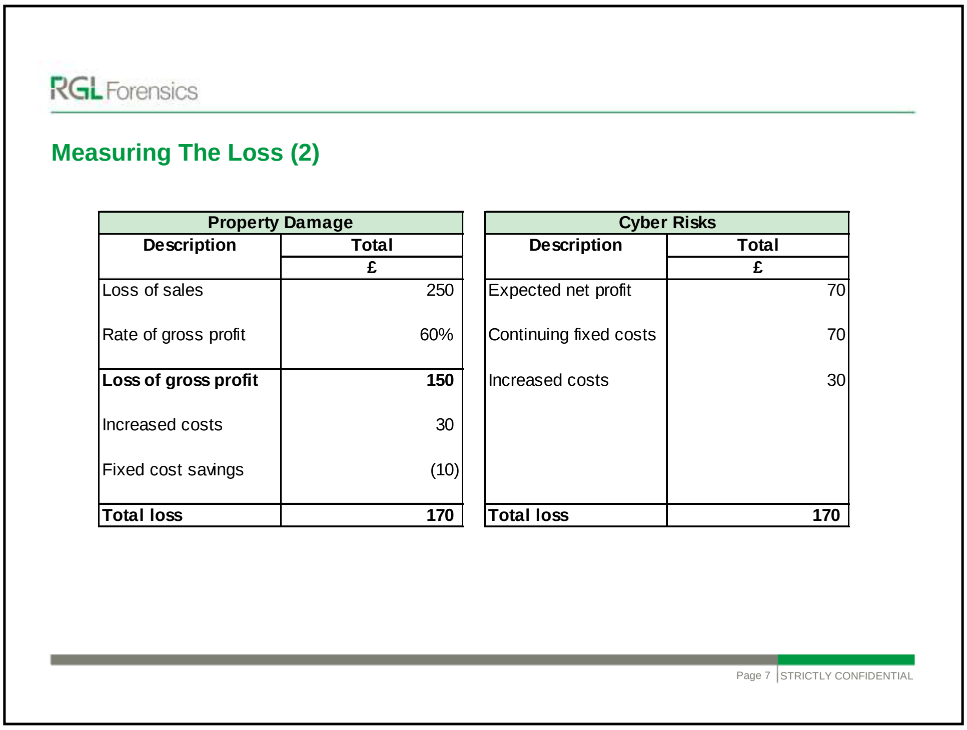
Defining Loss of Profits in Cyber Claims

- Reduction in net profit attributable to a loss of revenue arising from the incident
- Continuing operating expenses
- Increased costs of working solely incurred as a consequence of the incident to reduce the:
  - Length of the period of interruption
  - Loss of profit arising from the incident



Measuring The Loss (1)

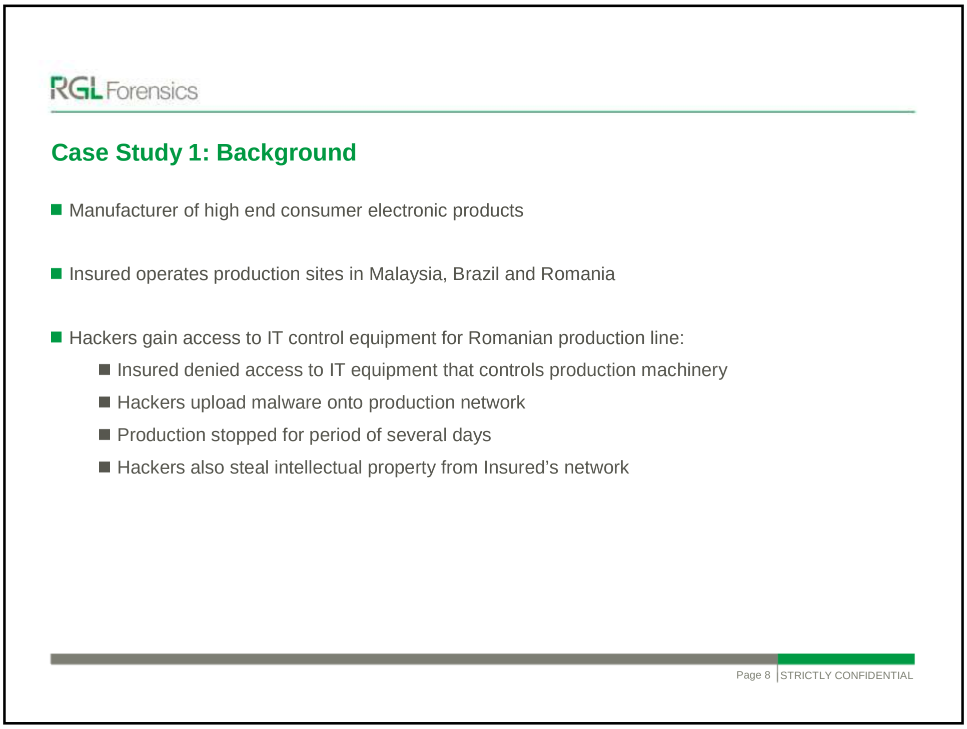
Expected But For Incident		Actual	
Description	Total	Description	Total
	£		£
Sales	250	Sales	125
Variable costs	(100)	Variable costs	(50)
Gross Profit	**150**	**Gross Profit**	**75**
Fixed costs	(80)	Fixed costs	(70)
		Increased costs	(30)
Net profit	**70**	**Net profit**	**(25)**



Measuring The Loss (2)

Property Damage	
Description	Total
	£
Loss of sales	250
Rate of gross profit	60%
Loss of gross profit	**150**
Increased costs	30
Fixed cost savings	(10)
Total loss	**170**

Cyber Risks	
Description	Total
	£
Expected net profit	70
Continuing fixed costs	70
Increased costs	30
Total loss	**170**



Case Study 1: Background

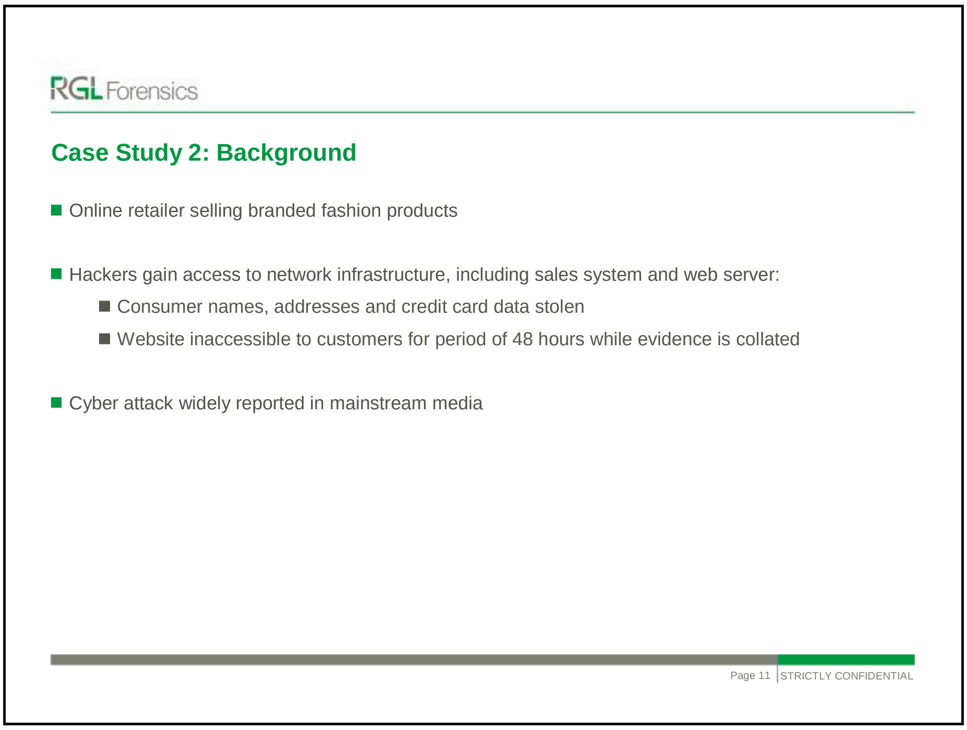
- Manufacturer of high end consumer electronic products
- Insured operates production sites in Malaysia, Brazil and Romania
- Hackers gain access to IT control equipment for Romanian production line:
  - Insured denied access to IT equipment that controls production machinery
  - Hackers upload malware onto production network
  - Production stopped for period of several days
  - Hackers also steal intellectual property from Insured’s network

Case Study 1: What Are The Issues?

- Length of time required to:
  - Regain control of the network and machinery
  - Repair hacker’s point of entry and remove malware
  - Restart production
  - Return production to pre-incident volumes
- Can production scheduling or location be amended to minimise sales losses?
- Risk of similar attack at other sites
- What intellectual property has been stolen and can it be recovered?

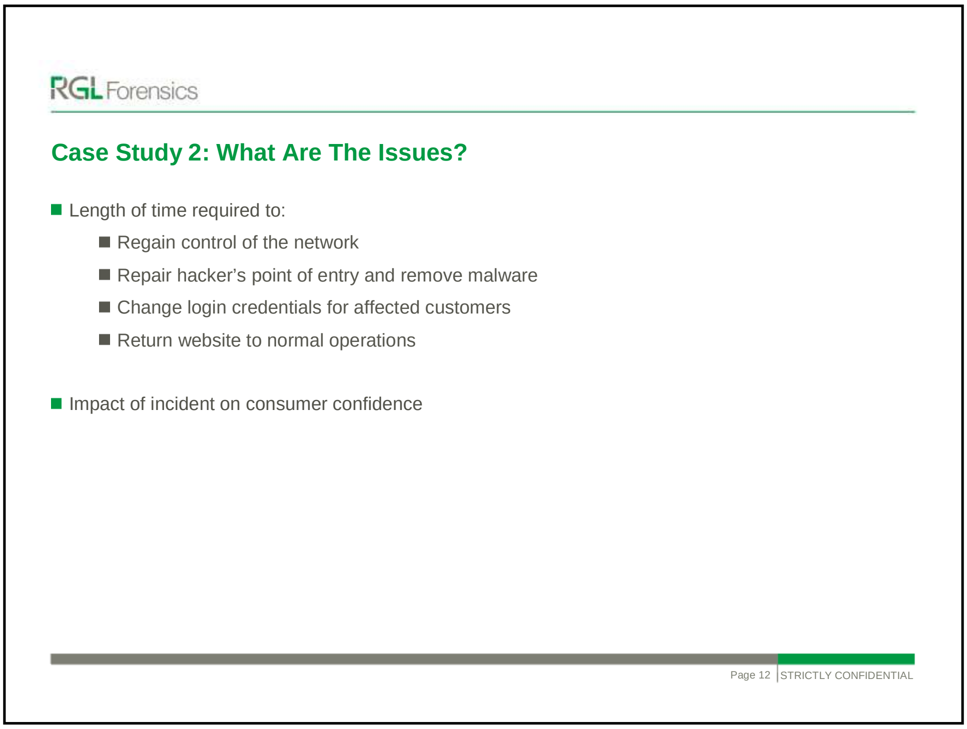
Case Study 1: Measuring The Loss

- Does loss of production cause a loss of sales?
  - Review pre and post incident production volumes at all relevant locations
  - Establish extent of production spare capacity, if any
  - Consider how stock volumes have been utilised
  - Analyse pre and post incident sales volumes for products manufactured on affected line
  - Review sales trends and market data for the relevant product
- Will theft of intellectual property cause a loss of revenue?
- Increased costs of working:
  - Overtime at incident and alternative locations during and after end of repair period
  - Airfreight costs for raw materials and finished goods
  - Outsourcing costs
- Savings may occur in shutdown period – e.g. energy, maintenance



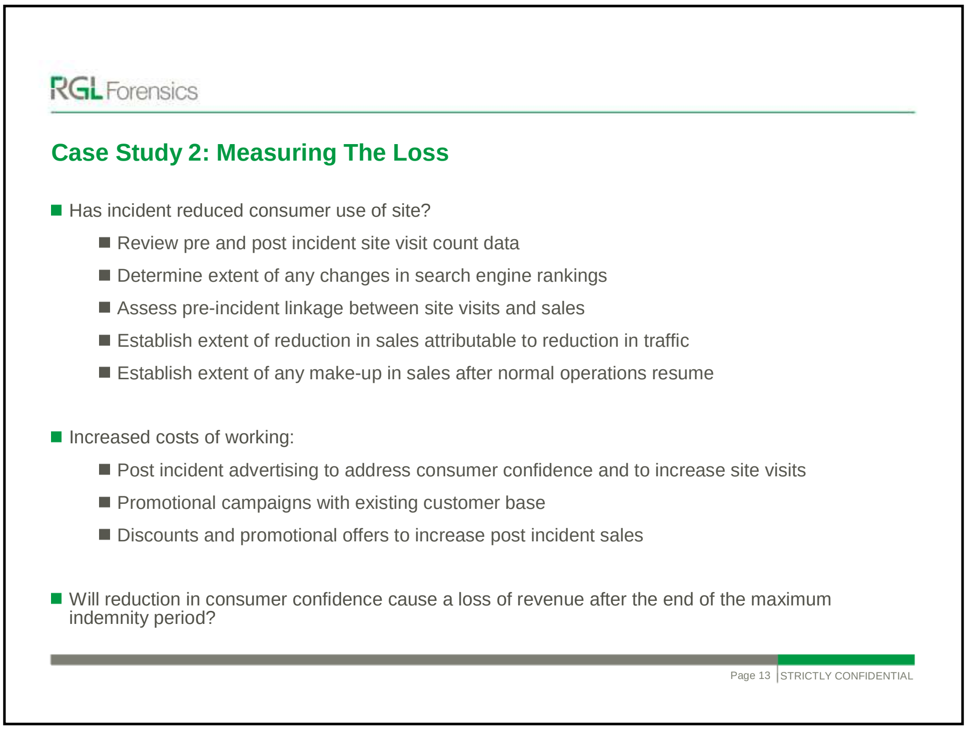
Case Study 2: Background

- Online retailer selling branded fashion products
- Hackers gain access to network infrastructure, including sales system and web server:
  - Consumer names, addresses and credit card data stolen
  - Website inaccessible to customers for period of 48 hours while evidence is collated
- Cyber attack widely reported in mainstream media



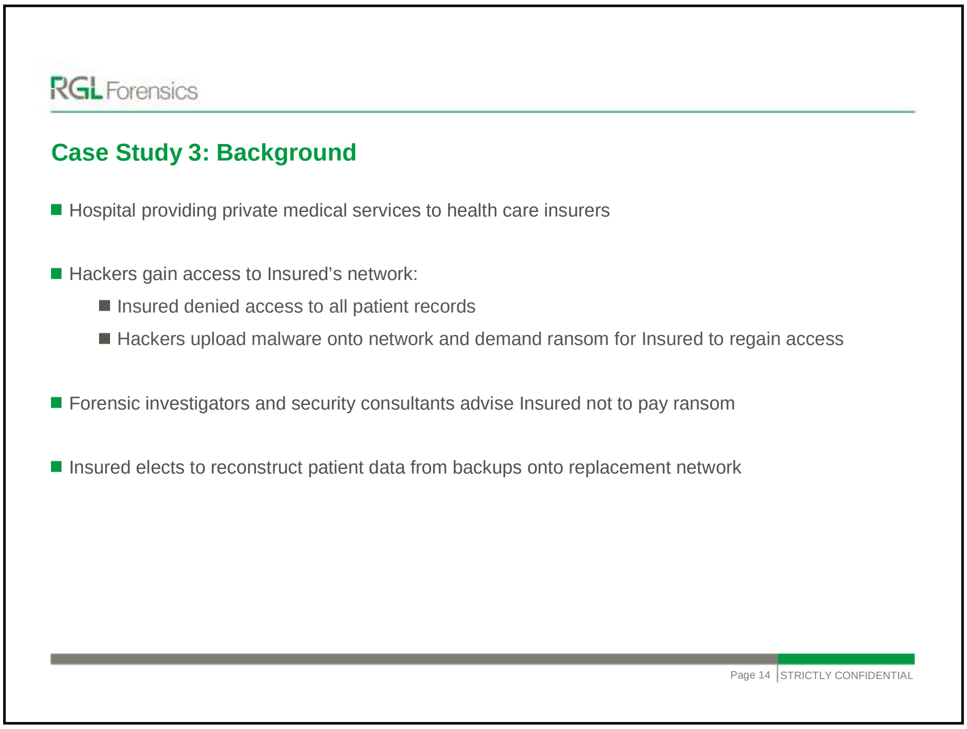
Case Study 2: What Are The Issues?

- Length of time required to:
  - Regain control of the network
  - Repair hacker’s point of entry and remove malware
  - Change login credentials for affected customers
  - Return website to normal operations
- Impact of incident on consumer confidence



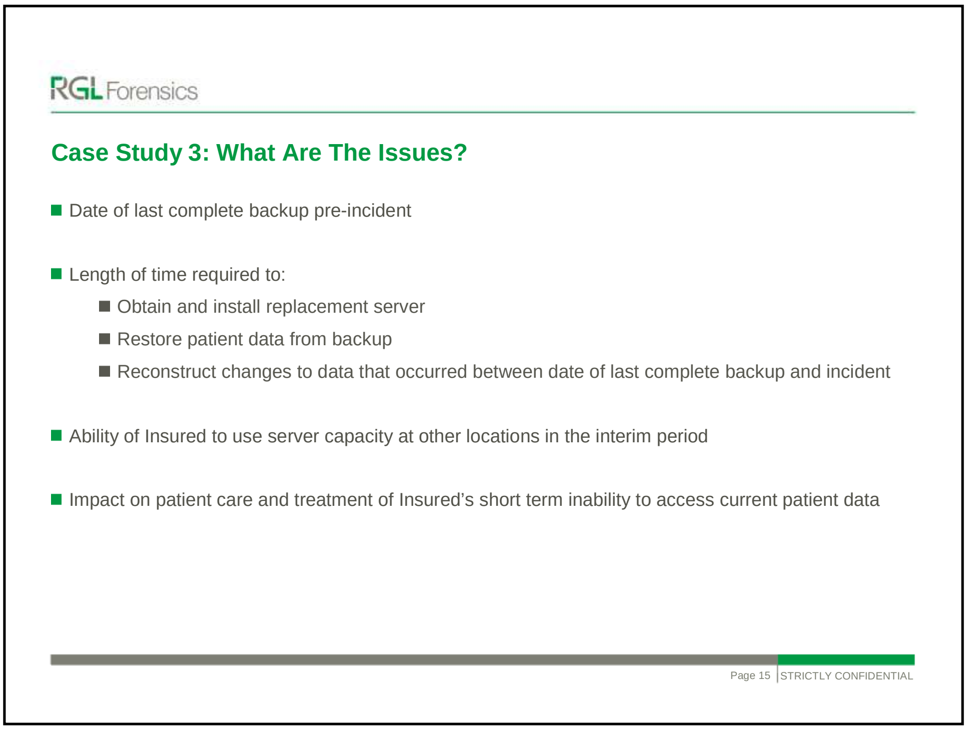
Case Study 2: Measuring The Loss

- Has incident reduced consumer use of site?
  - Review pre and post incident site visit count data
  - Determine extent of any changes in search engine rankings
  - Assess pre-incident linkage between site visits and sales
  - Establish extent of reduction in sales attributable to reduction in traffic
  - Establish extent of any make-up in sales after normal operations resume
- Increased costs of working:
  - Post incident advertising to address consumer confidence and to increase site visits
  - Promotional campaigns with existing customer base
  - Discounts and promotional offers to increase post incident sales
- Will reduction in consumer confidence cause a loss of revenue after the end of the maximum indemnity period?



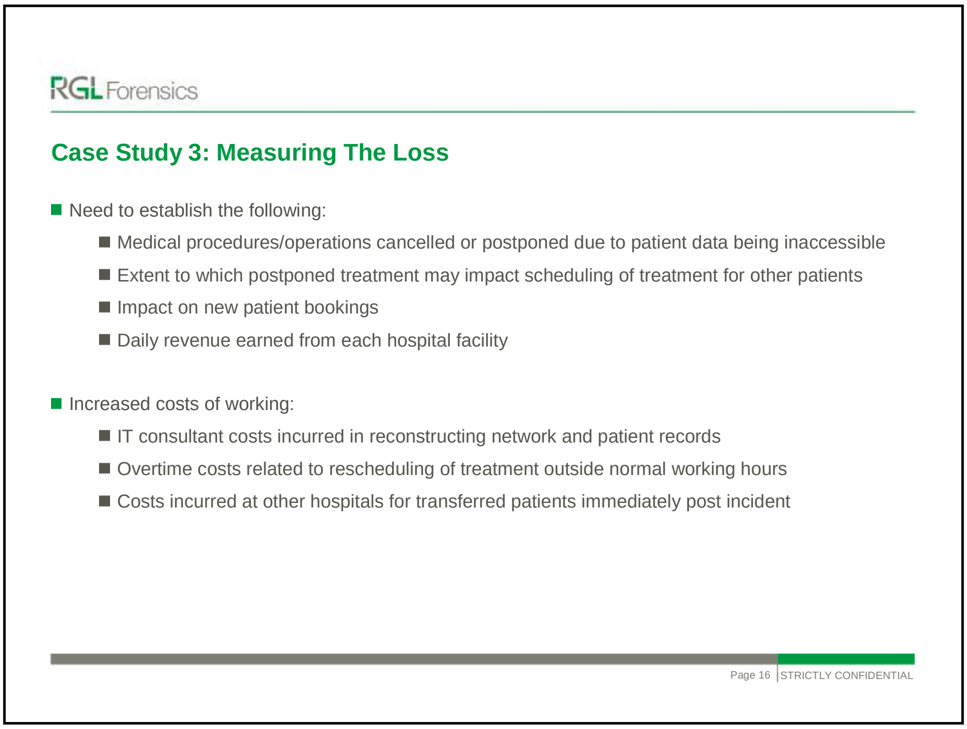
Case Study 3: Background

- Hospital providing private medical services to health care insurers
- Hackers gain access to Insured’s network:
  - Insured denied access to all patient records
  - Hackers upload malware onto network and demand ransom for Insured to regain access
- Forensic investigators and security consultants advise Insured not to pay ransom
- Insured elects to reconstruct patient data from backups onto replacement network



Case Study 3: What Are The Issues?

- Date of last complete backup pre-incident
- Length of time required to:
  - Obtain and install replacement server
  - Restore patient data from backup
  - Reconstruct changes to data that occurred between date of last complete backup and incident
- Ability of Insured to use server capacity at other locations in the interim period
- Impact on patient care and treatment of Insured’s short term inability to access current patient data



Case Study 3: Measuring The Loss

- Need to establish the following:
  - Medical procedures/operations cancelled or postponed due to patient data being inaccessible
  - Extent to which postponed treatment may impact scheduling of treatment for other patients
  - Impact on new patient bookings
  - Daily revenue earned from each hospital facility
- Increased costs of working:
  - IT consultant costs incurred in reconstructing network and patient records
  - Overtime costs related to rescheduling of treatment outside normal working hours
  - Costs incurred at other hospitals for transferred patients immediately post incident

Quantification Issues To Consider

- Issues may arise linking revenue losses to an incident given expectation of short interruption periods
- Indemnity period:
  - Assess potential for loss of sales to continue after repairs have completed
  - Consider potential for loss of sales to continue after end of maximum indemnity period
- Increased costs of working:
  - May be incurred to protect revenue before and after the end of the indemnity period
  - Proportion of total cost may therefore not be covered under the policy

Questions?