How Much Risk Does BYOD Represent?

Jack Jones - Principal, CXOWARE
Topics

• What’s your gut tell you?
• What does “risk” mean?
• To be FAIR about it...
• The analysis process
• Analysis results
• Reasonable questions...
• Summary
• Q&A
What's your gut tell you?

Just relying on your intuition and experience, how risky is BYOD?
What does “Risk” mean?

The probable frequency and probable magnitude of future loss.

(How often bad things are likely to happen, and how bad they’re likely to be.)

(“Loss Exposure”)

FAIR (in a nutshell)

- Factor Analysis of Information Risk (FAIR)
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)
• Purpose & Characteristics
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)
• Purpose & Characteristics
  – Framework for understanding and analyzing risk scenarios
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)

• Purpose & Characteristics
  – Framework for understanding and analyzing risk scenarios
  – Enables true quantitative analysis of risk
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)

• Purpose & Characteristics
  – Framework for understanding and analyzing risk scenarios
  – Enables true quantitative analysis of risk
  – Leverages proven methods
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)

• Purpose & Characteristics
  – Framework for understanding and analyzing risk scenarios
  – Enables true quantitative analysis of risk
  – Leverages proven methods
    • Bayesian networks
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)

• Purpose & Characteristics
  – Framework for understanding and analyzing risk scenarios
  – Enables true quantitative analysis of risk
  – Leverages proven methods
    • Bayesian networks
    • Monte Carlo analysis
FAIR (in a nutshell)

• Factor Analysis of Information Risk (FAIR)

• Purpose & Characteristics
  – Framework for understanding and analyzing risk scenarios
  – Enables true quantitative analysis of risk
  – Leverages proven methods
  • Bayesian networks
  • Monte Carlo analysis
  • Calibrated estimation
The FAIR taxonomy

- Risk
  - Loss Event Frequency
  - Loss Magnitude
The FAIR taxonomy
The FAIR taxonomy

Risk

Loss Event Frequency

Threat Event Frequency

Vulnerability

Loss Magnitude

Primary Loss

Secondary Loss
The FAIR taxonomy

- Risk
  - Loss Event Frequency
    - Threat Event Frequency
    - Vulnerability
  - Loss Magnitude
    - Primary Loss
    - Secondary Loss
      - Secondary Loss Event Frequency
      - Secondary Loss Magnitude
The FAIR taxonomy

- Risk – The probable frequency and probable magnitude of future loss
- Loss Event Frequency (LEF) – Annualized frequency of loss events
- Threat Event Frequency (TEF) – Annualized frequency of events where loss could result
- Vulnerability – The probability that a Threat Event becomes a Loss Event
- Loss Magnitude – The per-event magnitude of loss (combination of Primary and Secondary losses)
- Primary Loss – The per-event magnitude of loss that results directly from an event
- Secondary Loss – The magnitude of loss that results from secondary reactions to an event
- Secondary Loss Event Frequency – The probability that secondary stakeholders will react negatively to an event
- Secondary Loss Magnitude – The per-event magnitude of loss from secondary stakeholder reactions
Analysis process

• Define (model) the scenario
  – Basic conditions and assumptions
Analysis process

• Define (model) the scenario
  – Basic conditions and assumptions

• Gather data & estimates
  – Document sources, rationale, and assumptions
  – Refine the scenario definition (if necessary)
Analysis process

• **Define (model) the scenario**
  – Basic conditions and assumptions

• **Gather data & estimates**
  – Document sources, rationale, and assumptions
  – Refine the scenario definition (if necessary)

• **Derive risk**
More about assumptions...

- What were your assumptions when I asked about the level of risk BYOD represents?
  - Assets at risk?
  - Threat actors?
  - Attack vectors?
  - Controls?
More about assumptions...

• What were your assumptions when I asked about the level of risk BYOD represents?
  – Assets at risk?
  – Threat actors?
  – Attack vectors?
  – Controls?

• ALL risk analyses involve assumptions at some level
More about assumptions...

• What were your assumptions when I asked about the level of risk BYOD represents?
  – Assets at risk?
  – Threat actors?
  – Attack vectors?
  – Controls?

• ALL risk analyses involve assumptions at some level

• The key is recognizing assumptions that are key within your scenario
What are we trying to prevent?

• Compromise of customer information
• Compromise of corporate information
• Financial fraud
• Other...?
How might the loss occur?

• Loss/theft of the device
• Malware compromise
• Transmission interception
• Other...?
## Scenario table

<table>
<thead>
<tr>
<th></th>
<th>Device Loss/Theft</th>
<th>Malware Compromise</th>
<th>Transmission Interception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money (financial fraud)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Scenario table

<table>
<thead>
<tr>
<th></th>
<th>Device Loss/Theft</th>
<th>Malware Compromise</th>
<th>Transmission Interception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money (financial fraud)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Additional considerations...
## Scenario table

<table>
<thead>
<tr>
<th></th>
<th>Device Loss/Theft</th>
<th>Malware Compromise</th>
<th>Transmission Interception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Corporate information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money (financial fraud)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Additional considerations...**
  - BYOD access will be limited to e-mail
## Scenario table

<table>
<thead>
<tr>
<th></th>
<th>Device Loss/Theft</th>
<th>Malware Compromise</th>
<th>Transmission Interception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money (financial fraud)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Additional considerations...**
  - BYOD access will be limited to e-mail
  - Differentiate by type of device (e.g., iOS vs Android)?
## Scenario table

<table>
<thead>
<tr>
<th></th>
<th>Device Loss/ Theft</th>
<th>Malware Compromise</th>
<th>Transmission Interception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Corporate information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money (financial fraud)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Additional considerations...
- BYOD access will be limited to e-mail
- Differentiate by type of device (e.g., iOS vs Android)?
- Differentiate with/without an MDM solution?
Got data?
Gathering data

• What variables do we need to find data for?
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
    • Secondary loss event frequency
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
    • Secondary loss event frequency
    • Secondary loss magnitude
Gathering data

- **What variables do we need to find data for?**
  - Loss event frequency (or threat event frequency and vulnerability)
  - Primary loss
  - Secondary loss
    - Secondary loss event frequency
    - Secondary loss magnitude
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
    • Secondary loss event frequency
    • Secondary loss magnitude

• **What data do we have?**
Gathering data

• What variables do we need to find data for?
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
    • Secondary loss event frequency
    • Secondary loss magnitude

• What data do we have?
  – Loss history (frequency, impact, control conditions)
Gathering data

- **What variables do we need to find data for?**
  - Loss event frequency (or threat event frequency and vulnerability)
  - Primary loss
  - Secondary loss
  - Secondary loss event frequency
  - Secondary loss magnitude

- **What data do we have?**
  - Loss history (frequency, impact, control conditions)
  - Surface area and volume of PII at risk
Gathering data

• What variables do we need to find data for?
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
    • Secondary loss event frequency
    • Secondary loss magnitude

• What data do we have?
  – Loss history (frequency, impact, control conditions)
  – Surface area and volume of PII at risk
  – Control conditions
Gathering data

• **What variables do we need to find data for?**
  – Loss event frequency (or threat event frequency and vulnerability)
  – Primary loss
  – Secondary loss
    • Secondary loss event frequency
    • Secondary loss magnitude

• **What data do we have?**
  – Loss history (frequency, impact, control conditions)
  – Surface area and volume of PII at risk
  – Control conditions
  – The magnitude of loss when/if PII is compromised
Analysis input

• Loss event frequency
Analysis input

• Loss event frequency
  – 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
Analysis input

- **Loss event frequency**
  - 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
  - The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
Analysis input

- **Loss event frequency**
  - 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
  - The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
  - Estimated BYOD loss event frequency
Analysis input

• **Loss event frequency**
  - 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
  - The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
  - Estimated BYOD loss event frequency
    • Min: 10 yr
Analysis input

• **Loss event frequency**
  - 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
  - The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
  - Estimated BYOD loss event frequency
    • Min: 10 yr
    • Max: 25 yr
Analysis input

• Loss event frequency
  – 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
  – The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
  – Estimated BYOD loss event frequency
    • Min: 10 yr
    • Max: 25 yr
    • Most likely: 18 yr
Analysis input

• **Loss event frequency**
  - 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
  - The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
  - Estimated BYOD loss event frequency
    - Min: 10 yr
    - Max: 25 yr
    - Most likely: 18 yr
Analysis input

- **Asset surface area**
  - Review of sensitive customer information in e-mail found:
Analysis input

• Asset surface area
  – Review of sensitive customer information in e-mail found:
    • 7% of colleagues had sensitive customer information in e-mail
Analysis input

• Asset surface area
  – Review of sensitive customer information in e-mail found:
    • 7% of colleagues had sensitive customer information in e-mail
    • The volume of sensitive customer information per colleague:
Analysis input

• **Asset surface area**
  – Review of sensitive customer information in e-mail found:
    • 7% of colleagues had sensitive customer information in e-mail
    • The volume of sensitive customer information per colleague:
      – Min: 1 sensitive record
Analysis input

- **Asset surface area**
  - Review of sensitive customer information in e-mail found:
    - 7% of colleagues had sensitive customer information in e-mail
    - The volume of sensitive customer information per colleague:
      - Min: 1 sensitive record
      - Max: 50,000 sensitive records (spreadsheets)
Analysis input

• Asset surface area
  – Review of sensitive customer information in e-mail found:
    • 7% of colleagues had sensitive customer information in e-mail
    • The volume of sensitive customer information per colleague:
      – Min: 1 sensitive record
      – Max: 50,000 sensitive records (spreadsheets)
      – Mode: 35 sensitive records
Analysis input

• Asset surface area
  – Review of sensitive customer information in e-mail found:
    • 7% of colleagues had sensitive customer information in e-mail
    • The volume of sensitive customer information per colleague:
      – Min: 1 sensitive record
      – Max: 50,000 sensitive records (spreadsheets)
      – Mode: 35 sensitive records
    – These values play a role in:
Analysis input

• **Asset surface area**
  
  – Review of sensitive customer information in e-mail found:
    
    • 7% of colleagues had sensitive customer information in e-mail
    
    • The volume of sensitive customer information per colleague:
      
      – Min: 1 sensitive record
      
      – Max: 50,000 sensitive records (spreadsheets)
      
      – Mode: 35 sensitive records

  – These values play a role in:
    
    • The probability that a lost/stolen device would contain customer information in e-mail
Analysis input

• **Asset surface area**
  – Review of sensitive customer information in e-mail found:
    • 7% of colleagues had sensitive customer information in e-mail
    • The volume of sensitive customer information per colleague:
      – Min: 1 sensitive record
      – Max: 50,000 sensitive records (spreadsheets)
      – Mode: 35 sensitive records
  – These values play a role in:
    • The probability that a lost/stolen device would contain customer information in e-mail
    • The probable volume of exposed customer records, which drives various forms of loss
Analysis input

• Loss magnitude
Analysis input

• Loss magnitude
  – Primary loss
Analysis input

• **Loss magnitude**
  
  – **Primary loss**
    
    • Comprised of person-hours responding to the event ($100 hr) and/or lost revenue
Analysis input

• Loss magnitude
  – Primary loss
    • Comprised of person-hours responding to the event ($100 hr) and/or lost revenue
      – Min: $100
Analysis input

- **Loss magnitude**
  - **Primary loss**
    - Comprised of person-hours responding to the event ($100/hr) and/or lost revenue
      - Min: $100
      - Max: $25,000 (includes lost revenue and response person-hours)
Analysis input

• Loss magnitude
  – Primary loss
    • Comprised of person-hours responding to the event ($100 hr) and/or lost revenue
      – Min: $100
      – Max: $25,000 (includes lost revenue and response person-hours)
      – ML: $240
Analysis input

• Loss magnitude
  – Primary loss
    • Comprised of person-hours responding to the event ($100/hr) and/or lost revenue
      – Min: $100
      – Max: $25,000 (includes lost revenue and response person-hours)
      – ML: $240
  – Secondary loss event frequency
Analysis input

• **Loss magnitude**
  
  – **Primary loss**
    
    • Comprised of person-hours responding to the event ($100 hr) and/or lost revenue
      
      – Min: $100
      
      – Max: $25,000 (includes lost revenue and response person-hours)
      
      – ML: $240

  – **Secondary loss event frequency**
    
    • Driven by the probability that a device will contain sensitive customer information (7%). Because that percentage may vary over time:
Analysis input

• Loss magnitude
  
  – Primary loss
    
    • Comprised of person-hours responding to the event ($100 hr) and/or lost revenue
      
      – Min: $100
      
      – Max: $25,000 (includes lost revenue and response person-hours)
      
      – ML: $240
  
  – Secondary loss event frequency
    
    • Driven by the probability that a device will contain sensitive customer information (7%). Because that percentage may vary over time:
      
      – Min: 5%
Analysis input

- **Loss magnitude**
  - Primary loss
    - Comprised of person-hours responding to the event ($100/hr) and/or lost revenue
      - Min: $100
      - Max: $25,000 (includes lost revenue and response person-hours)
      - ML: $240
  - Secondary loss event frequency
    - Driven by the probability that a device will contain sensitive customer information (7%). Because that percentage may vary over time:
      - Min: 5%
      - Max: 10%
Analysis input

• Loss magnitude
  – Primary loss
    • Comprised of person-hours responding to the event ($100 hr) and/or lost revenue
      – Min: $100
      – Max: $25,000 (includes lost revenue and response person-hours)
      – ML: $240
  – Secondary loss event frequency
    • Driven by the probability that a device will contain sensitive customer information (7%). Because that percentage may vary over time:
      – Min: 5%
      – Max: 10%
      – ML: 7%
Analysis input

- Loss magnitude
Analysis input

• Loss magnitude
  – Secondary loss magnitude
Analysis input

- **Loss magnitude**
  - Secondary loss magnitude
    - Largely tied to volume of exposed records
Analysis input

• Loss magnitude
  – Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
Analysis input

- **Loss magnitude**
  - Secondary loss magnitude
    - Largely tied to volume of exposed records
    - Response (notifications, credit monitoring, legal defense, CIRT)
      - Notification: $5 per affected customer
Analysis input

• Loss magnitude
  – Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      – Notification: $5 per affected customer
      – Credit monitoring: $25 per affected customer
Analysis input

• **Loss magnitude**
  - Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      – Notification: $5 per affected customer
      – Credit monitoring: $25 per affected customer
      – CIRT logistics:
Analysis input

- **Loss magnitude**
  - Secondary loss magnitude
    - Largely tied to volume of exposed records
    - Response (notifications, credit monitoring, legal defense, CIRT)
      - Notification: $5 per affected customer
      - Credit monitoring: $25 per affected customer
      - CIRT logistics:
        » Min: $2k (20 person-hours)
Analysis input

• Loss magnitude
  – Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      – Notification: $5 per affected customer
      – Credit monitoring: $25 per affected customer
      – CIRT logistics:
        » Min: $2k (20 person-hours)
        » Max: $50k (500 person-hours)
Analysis input

• Loss magnitude
  – Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      – Notification: $5 per affected customer
      – Credit monitoring: $25 per affected customer
      – CIRT logistics:
        » Min: $2k (20 person-hours)
        » Max: $50k (500 person-hours)
        » ML: $3.5k (35 person-hours)
Analysis input

• Loss magnitude
  – Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      – Notification: $5 per affected customer
      – Credit monitoring: $25 per affected customer
      – CIRT logistics:
        » Min: $2k (20 person-hours)
        » Max: $50k (500 person-hours)
        » ML: $3.5k (35 person-hours)
      – Legal defense
Analysis input

- **Loss magnitude**
  - Secondary loss magnitude
    - Largely tied to volume of exposed records
    - Response (notifications, credit monitoring, legal defense, CIRT)
      - Notification: $5 per affected customer
      - Credit monitoring: $25 per affected customer
      - CIRT logistics:
        - Min: $2k (20 person-hours)
        - Max: $50k (500 person-hours)
        - ML: $3.5k (35 person-hours)
    - Legal defense
      - Min: $0 (best-case no legal action results)
Analysis input

• Loss magnitude
  – Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      – Notification: $5 per affected customer
      – Credit monitoring: $25 per affected customer
      – CIRT logistics:
        » Min: $2k (20 person-hours)
        » Max: $50k (500 person-hours)
        » ML: $3.5k (35 person-hours)
      – Legal defense
        » Min: $0 (best-case no legal action results)
        » Max: $500k (class action defense costs)
Analysis input

• **Loss magnitude**
  - Secondary loss magnitude
    • Largely tied to volume of exposed records
    • Response (notifications, credit monitoring, legal defense, CIRT)
      - Notification: $5 per affected customer
      - Credit monitoring: $25 per affected customer
      - CIRT logistics:
        » Min: $2k (20 person-hours)
        » Max: $50k (500 person-hours)
        » ML: $3.5k (35 person-hours)
    - Legal defense
      » Min: $0 (best-case no legal action results)
      » Max: $500k (class action defense costs)
      » ML: $0 (assumes no legal action from a compromise of 35 customer records)
Analysis input

- Loss magnitude
Analysis input

• Loss magnitude
  – Secondary loss magnitude - continued
Analysis input

• **Loss magnitude**
  – Secondary loss magnitude - continued
    • Fines and Judgments
Analysis input

• Loss magnitude
  – Secondary loss magnitude - continued
    • Fines and Judgments
      – Min: $0
Analysis input

• **Loss magnitude**
  – Secondary loss magnitude - continued
    • **Fines and Judgments**
      – Min: $0
      – Max: $1M (primarily reflects regulatory actions)
Analysis input

• **Loss magnitude**
  - Secondary loss magnitude - continued
    • **Fines and Judgments**
      - Min: $0
      - Max: $1M (primarily reflects regulatory actions)
      - ML: $0
Analysis input

• **Loss magnitude**
  
  – Secondary loss magnitude - continued
    
    • **Fines and Judgments**
      
      – Min: $0
      
      – Max: $1M (primarily reflects regulatory actions)
      
      – ML: $0
    
    • **Reputation damage**
Analysis input

• Loss magnitude
  – Secondary loss magnitude - continued
    • Fines and Judgments
      – Min: $0
      – Max: $1M (primarily reflects regulatory actions)
      – ML: $0
    • Reputation damage
      – Materialized through reduced market share, reduced stock price, and/or increased cost of capital
Analysis input

• **Loss magnitude**
  - Secondary loss magnitude - continued
    • Fines and Judgments
      - Min: $0
      - Max: $1M (primarily reflects regulatory actions)
      - ML: $0
    • Reputation damage
      - Materialized through reduced market share, reduced stock price, and/or increased cost of capital
      - Note that even the max breach size is not expected to affect stock price or cost of capital
Analysis input

• Loss magnitude
  – Secondary loss magnitude - continued
    • Fines and Judgments
      – Min: $0
      – Max: $1M (primarily reflects regulatory actions)
      – ML: $0
    • Reputation damage
      – Materialized through reduced market share, reduced stock price, and/or increased cost of capital
      – Note that even the max breach size is not expected to affect stock price or cost of capital
        » Min: $0
Analysis input

• **Loss magnitude**
  
  – Secondary loss magnitude - continued
  
  • **Fines and Judgments**
    
    – Min: $0
    
    – Max: $1M (primarily reflects regulatory actions)
    
    – ML: $0
  
  • **Reputation damage**
    
    – Materialized through reduced market share, reduced stock price, and/or increased cost of capital
    
    – Note that even the max breach size is not expected to affect stock price or cost of capital
      
      » Min: $0
      
      » Max: $75k
Analysis input

• Loss magnitude
  – Secondary loss magnitude - continued
    • Fines and Judgments
      – Min: $0
      – Max: $1M (primarily reflects regulatory actions)
      – ML: $0
    • Reputation damage
      – Materialized through reduced market share, reduced stock price, and/or increased cost of capital
      – Note that even the max breach size is not expected to affect stock price or cost of capital
        » Min: $0
        » Max: $75k
        » ML: $3.5k
Computing your results.............
Individual analysis results

- Annualized loss exposure for device loss/theft where customer PII is at risk...

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Mode</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total Loss Exposure</strong></td>
<td>$6,500</td>
<td>$62,000</td>
<td>$39,000</td>
<td>$300,000</td>
</tr>
</tbody>
</table>

Example only – your results WILL differ!
### Aggregate analysis results

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Min</th>
<th>Avg</th>
<th>Mode</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss/Theft – PII</td>
<td>$6500</td>
<td>$62,000</td>
<td>$39,000</td>
<td>$300,000</td>
</tr>
<tr>
<td>Malware – PII</td>
<td>$16,000</td>
<td>$150,000</td>
<td>$98,000</td>
<td>$750,000</td>
</tr>
<tr>
<td>Transmission – PII</td>
<td>$1200</td>
<td>$2,500</td>
<td>$1,900</td>
<td>$57,000</td>
</tr>
<tr>
<td>Loss/Theft – Corp Data</td>
<td>$300</td>
<td>$600</td>
<td>$400</td>
<td>$43,000</td>
</tr>
<tr>
<td>Malware – Corp Data</td>
<td>$450</td>
<td>$1,100</td>
<td>$900</td>
<td>$65,000</td>
</tr>
<tr>
<td>Transmission – Corp Data</td>
<td>$100</td>
<td>$250</td>
<td>$200</td>
<td>$12,000</td>
</tr>
<tr>
<td>Loss/Theft – Financial Fraud</td>
<td>$100</td>
<td>$300</td>
<td>$150</td>
<td>$9,000</td>
</tr>
<tr>
<td>Malware – Financial Fraud</td>
<td>$150</td>
<td>$400</td>
<td>$300</td>
<td>$5000</td>
</tr>
<tr>
<td>Transmission – Financial Fraud</td>
<td>$50</td>
<td>$200</td>
<td>$100</td>
<td>$1200</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$24,850</strong></td>
<td><strong>$217,350</strong></td>
<td><strong>$140,950</strong></td>
<td><strong>$1,242,200</strong></td>
</tr>
</tbody>
</table>

Example only – your results WILL differ!
Comparing with/without an MDM product

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Min</th>
<th>Avg</th>
<th>Mode</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without MDM</td>
<td>$25,000</td>
<td>$217,000</td>
<td>$141,000</td>
<td>$1,200,000</td>
</tr>
<tr>
<td>With MDM</td>
<td>$6,000</td>
<td>$55,000</td>
<td>$30,000</td>
<td>$350,000</td>
</tr>
<tr>
<td>Difference</td>
<td>$19,000</td>
<td>$162,000</td>
<td>$111,000</td>
<td>$850,000</td>
</tr>
</tbody>
</table>

Example only – your results WILL differ!
Reasonable questions...

• Isn’t the input subjective?
Reasonable questions...

- Isn’t the input subjective?
- Couldn’t someone else do the analysis and come up with a different answer?
Reasonable questions...

- Isn’t the input subjective?
- Couldn’t someone else do the analysis and come up with a different answer?
- Why is the output imprecise?
Reasonable questions...

- Isn’t the input subjective?
- Couldn’t someone else do the analysis and come up with a different answer?
- Why is the output imprecise?
- Won’t executives always accept the risk?
Conclusions

• There’s no single answer regarding BYOD risk, but you can do analysis that will tell you how much risk it represents to your organization
Conclusions

• There’s no single answer regarding BYOD risk, but you can do analysis that will tell you how much risk it represents to your organization.

• The amount of risk BYOD introduces depends on which scenarios are relevant to your organization, as well as your specific variables.
Conclusions

• There’s no single answer regarding BYOD risk, but you can do analysis that will tell you how much risk it represents to your organization.

• The amount of risk BYOD introduces depends on which scenarios are relevant to your organization, as well as your specific variables.

• Good risk analysis relies on
Conclusions

• There’s no single answer regarding BYOD risk, but you can do analysis that will tell you how much risk it represents to your organization

• The amount of risk BYOD introduces depends on which scenarios are relevant to your organization, as well as your specific variables

• Good risk analysis relies on
  – Effective scenario definition
Conclusions

• There’s no single answer regarding BYOD risk, but you can do analysis that will tell you how much risk it represents to your organization.

• The amount of risk BYOD introduces depends on which scenarios are relevant to your organization, as well as your specific variables.

• Good risk analysis relies on
  – Effective scenario definition
  – Recognizing and leveraging data sources.
Conclusions

• There’s no single answer regarding BYOD risk, but you can do analysis that will tell you how much risk it represents to your organization

• The amount of risk BYOD introduces depends on which scenarios are relevant to your organization, as well as your specific variables

• Good risk analysis relies on
  – Effective scenario definition
  – Recognizing and leveraging data sources
  – Appropriately leveraging subject matter experts
Questions?