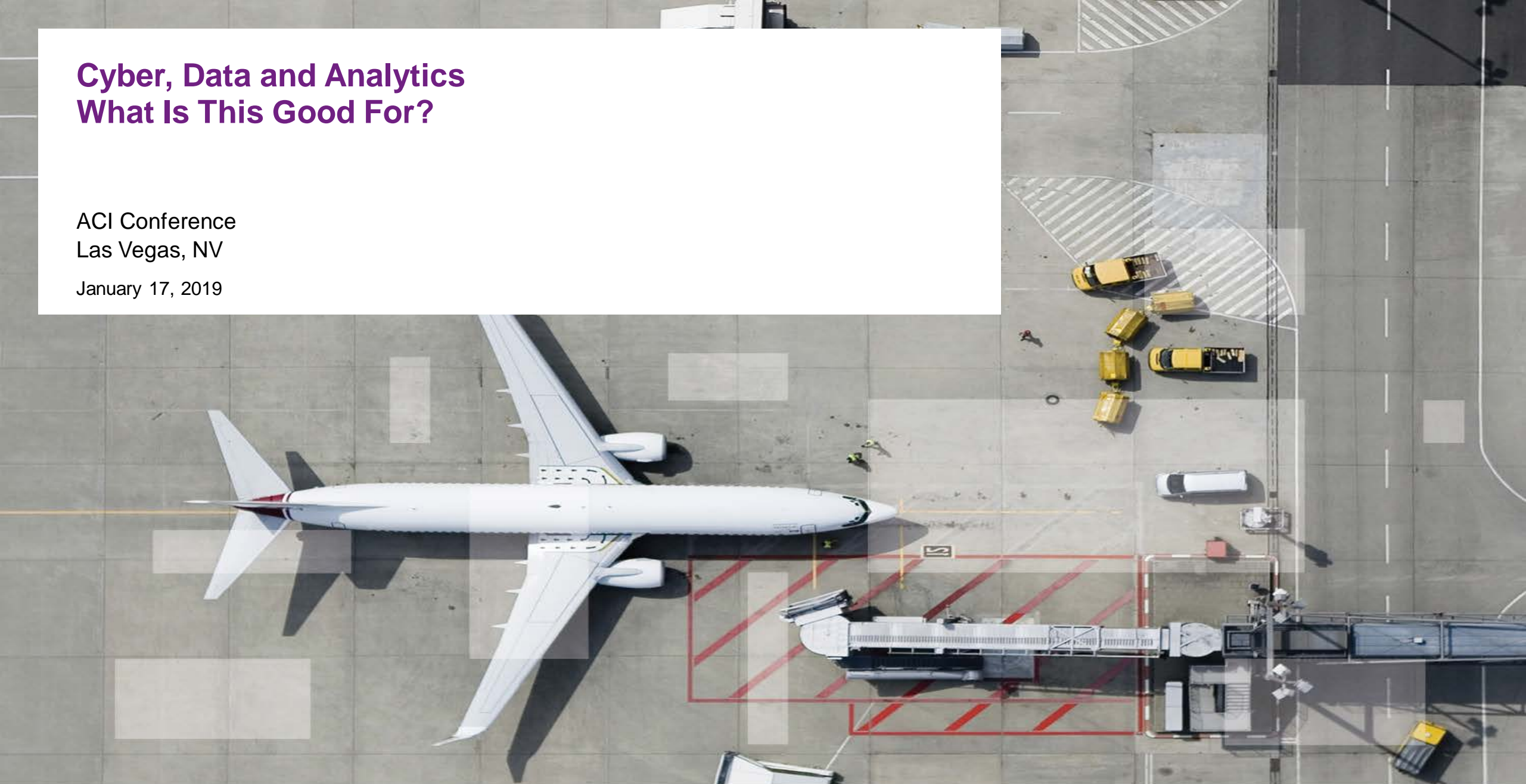


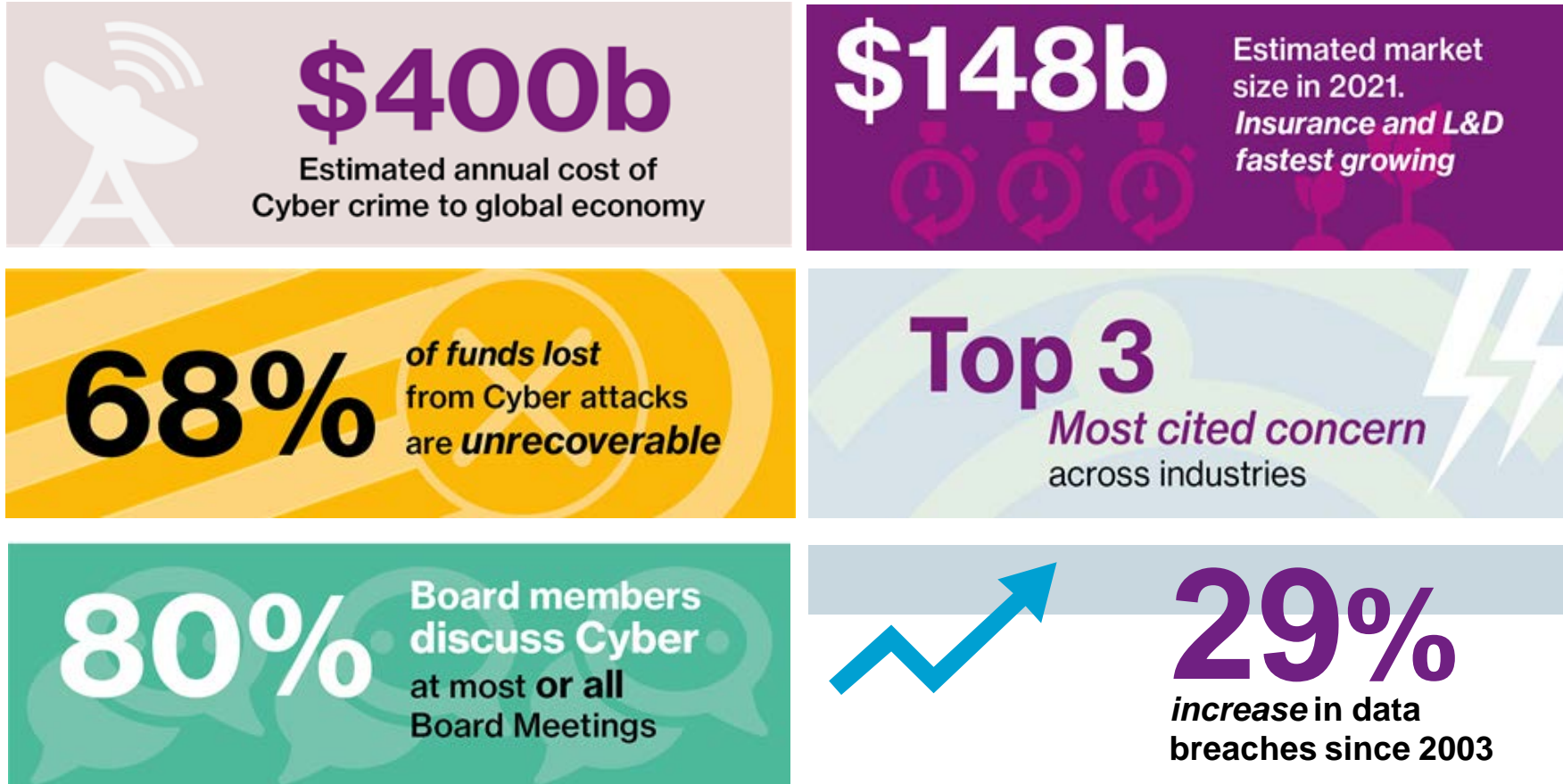
Cyber, Data and Analytics What Is This Good For?

ACI Conference
Las Vegas, NV
January 17, 2019



Prevalence of cyber crime in business – financial impact

Some evidence:



Source: Federal Government Resources

Prevalence of cyber crime in business – threat

4,000
Ransomware attacks per day in 2016

93% cases - attackers took minutes or less to compromise systems

70% breaches involving insider misuse took months or years to discover
83% cases – organizations took weeks or more to discover breaches

62
New ransomware families detected

11 Fold Increase
new modifications
Q1 2,900
Q3 32,091

Businesses attacked
Q1 Every two minutes
Q3 Every 40 seconds

Individuals attacked:
Q1 Every 20 seconds
Q3 Every 10 seconds

\$1Billion crime:
4,000 attacks daily

Email:
Phishing **#1**
distribution method

How does this happen?

It just takes one click...

As evidenced by the recent WannaCry incident, attacks often start with an email message containing an attachment or a link to a website then quietly installs the malicious software.

Source: Antivirus Software Companies – 2016 statistics

NotPetya Global Attack: Financial and Operational Impacts

**7 firms
in 5
industries**



Pharmaceutical



or more
through
year end
2017

Disruption of worldwide operations, including manufacturing, research and sales operations.



Logistics/Shipping



impact on **results**

Significant impact to worldwide operations and communications.



impact on **profitability**

Lost volumes as well as extraordinary costs in IT and operations.



Consumer Goods

Estimated
3Q17



Protracted period required to restore some systems resulted in a backlog in supply system processes.



through
3Q17

The malware affected a significant portion of company's global sales, distribution and financial networks.



Construction

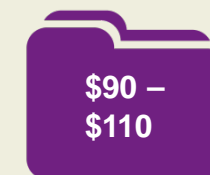


lost
sales
by year
end

Downtime of IT systems and supply chain disruptions.



Technology



million

Malware affected company systems to receive and process orders.

The Cyber Claims Experience - Your Peers

Ransomware events

- At Beazley, we've seen ransomware events double year-over-year, and then do so again
- Transit Systems (San Francisco MUNI; ransomware; approx. 2 days of lost transit revenue; Nov. 2016)
- Ports (Port of San Diego; permits, business services, public records impacted; Fall 2018)
- Municipal Systems (Atlanta; March 2018)

Hacks (for private information or for money)

- Hacks create multiple exposures
- City Transit Authority (Payroll redirect)
- State transportation department (employee and former employee personnel information)

Airport Cyber Risk: The Claims Experience

**1,000 attacks per month on aviation sector
(European Aviation Safety Agency 2018)**

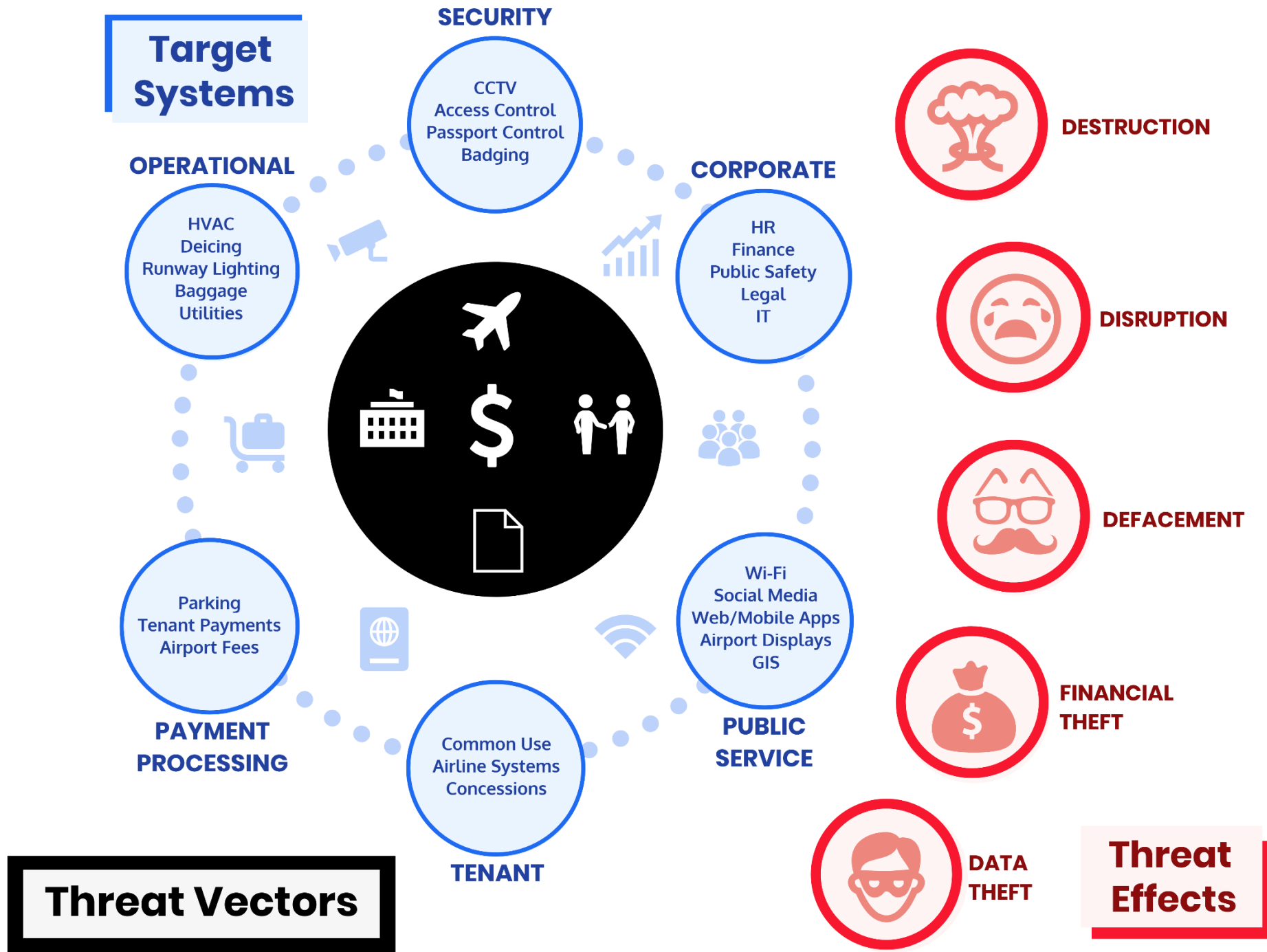
- **The ransomware event**
- **The email compromise**
- **The cloud services incident**
- **The system failure**



City of Atlanta

Hartsfield-Jackson Atlanta International Airport

- Ransomware Attack – March 2018
 - Ongoing Cyber Claim
 - Airport not Impacted
- Separate Cyber policies for City and Airport
 - Different exposures



Measuring Your Exposure – Claims Considerations

To measure your cyber exposure, consider:

- Privacy risk
- Liability risk
- Business interruption risk
- Vendor risk









Test your Cyber Incident Response and Business Continuity Plans

Identify critical assets and systems

Don't Forget Your External Third-Party Relationships

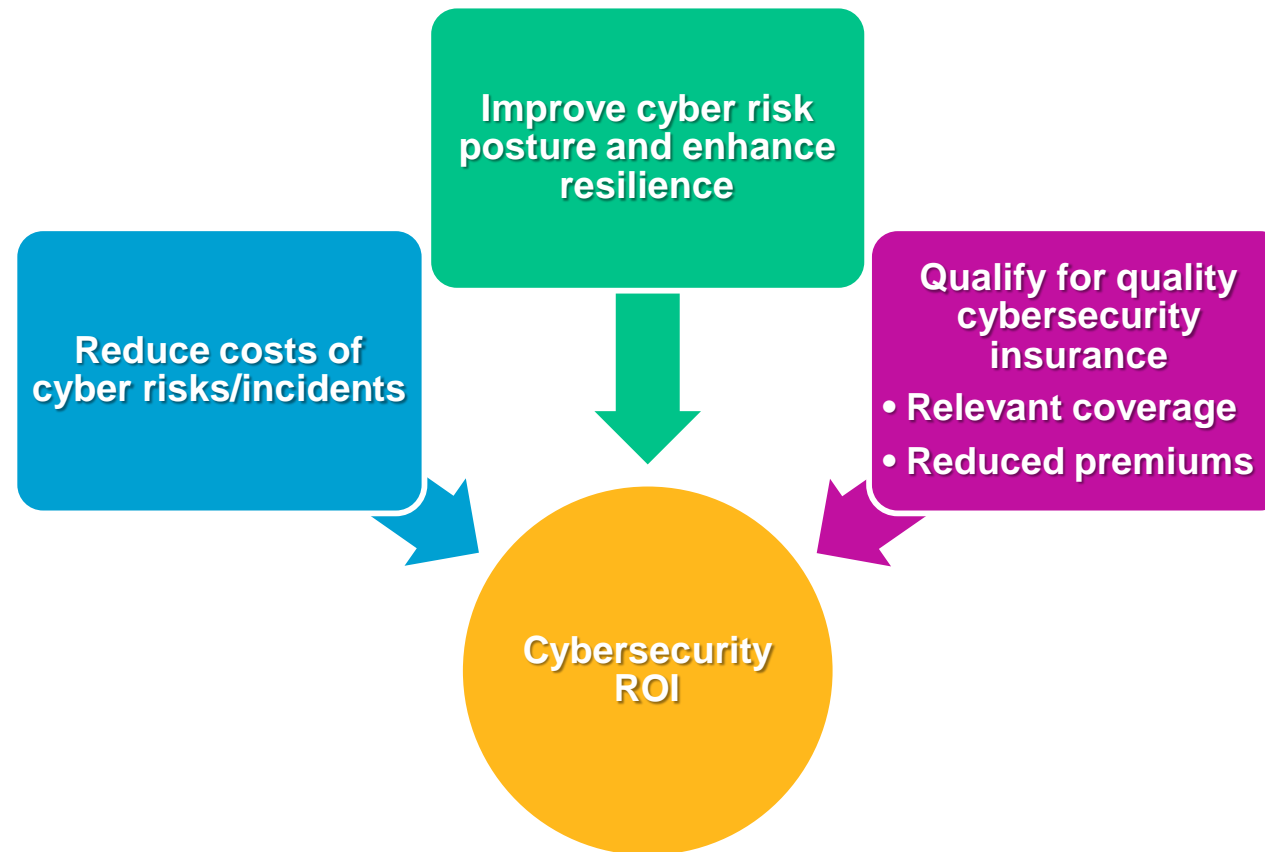
European General Data Protection Regulation (GDPR) Summary

On April 14, 2016 the European Parliament voted to adopt a new data protection law for Europe: the General Data Protection Regulation (GDPR). The GDPR presents the most ambitious and comprehensive changes to data protection rules around the world in the last 20 years and will apply to almost all private sector processing by organizations in the EU or by organizations outside the EU targeting EU residents. Data protection guidelines will be significantly tightened, individuals' rights (including to bring claims) will be strengthened and fines for a breach of the law could be for as high as 4% of global annual revenues. The Regulation took effect on May 25, 2018, and impacts all business sectors. Organizations should have already assessed how the Regulation will change their current data protection compliance obligations.

 Increased enforcement powers The Regulation will significantly increase the maximum fine for breaching the data protection law to €20 million, or 2-4% of global annual revenues, whichever is greater.	 Strict data breach notification laws The Regulation will require businesses to notify data breaches within <u>72 hours</u> where there is risk to affected individuals.
 New obligations of data processors The Regulation imposes obligations directly on data processors who will also be subject to enforcement actions. Processors, such as cloud providers, will be subject to fines up to the same levels as controllers if they breach their obligations.	 The 'right to be forgotten' Individuals will have an expanded right to request that businesses delete their personal data in certain circumstances (e.g. the data is no longer necessary for the purpose for which it was collected).
 Expanded territorial scope Non-EU businesses will be subject to the regulation if they: (i) offer goods or services to data subjects in the EU; or (ii) monitor data subjects' behaviour in the EU.	 The right to object to profiling Individuals will have the right not to be subjected to profiling that 'significantly' affects them.
 Consent, as a legal basis for processing, will be harder to obtain Consent must be freely given, specific, informed and unambiguous, and demonstrated either by a statement or a clear affirmative action.	 The right to data portability The Regulation will give data subjects the right to obtain a copy of their personal data from the data controller in a commonly used format
 Privacy by design and by default Businesses will be required to implement data protection by design (e.g. when creating new products, services or other data processing activities) and by default (e.g. data minimisation). Businesses will also be required to perform data protection impact assessments to identify and address privacy risks in new products	 Risk-based approach to compliance Businesses will be responsible for assessing the degree of risk that their processing activities pose to data subjects, and for implementing appropriate measures to ensure compliance.
 Greater harmonization The Regulation will introduce a single legal framework that applies across all EU member states.	 The 'one-stop shop' The Regulation will introduce a single legal framework that applies across all EU member states.
 Binding corporate rules BCRs are agreements used to lawfully transfer personal data out of the European Economic Area. The Regulation will formally recognise BCRs.	 'Pseudonymisation' Data that can no longer be attributed to a specific individual, such as key-coded data, will still amount to personal data, but may be subject to fewer restrictions on processing, provided that the risk of harm is low.

Why a Holistic Approach to Cyber Risk Management?

Enabling decision making to attain the greatest ROI on cyber security investment



Information Security Countermeasures

Reduce costs of cyber risks/incidents

- Manage and protect your sensitive operations and data
- Transfer risk to vendors whenever possible
- Control access and permissions
- Do a security cost/benefit analysis for new apps, systems, and features
- Continually assess and remediate security gaps

Improve cyber risk posture and enhance resilience

- Segment systems and applications
- Build in redundancy, system backup, and restoral
- Invest in a Few Good (Security) Tools
- Exercise and refine your Incident Response processes
- Educate and involve the entire business



Cyber Security and Risk Management

- Government/Municipality – limited resources
- ERM Philosophy – assessment of organizational exposures
- Forward Thinking CISO
 - IT Security Governance Board
 - Participation from all stakeholders
 - Citywide IT Risk Assessment – Frameworks/Tools
 - NIST (National Institute of Standards and Technology, a unit of the US Dept of Commerce)
 - <https://www.nist.gov>
 - ISO 31000 (International Organization for Standardization)
 - <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>
 - CSET® (Cyber Security Evaluation Tool, a Department of Homeland Security product)
 - <https://cset.inl.gov>

So now you want insurance.....

How does insurance create value and how do we determine that value?

Premium typically exceeds expected transferred losses for the policy period

This does not mean that insurance does not provide value. Transferring loss and its corresponding volatility has benefits:

- Reducing cash flow uncertainty
- Preventing liquidity issues
- Due diligence of the board and senior managers



The solution - Cyber Liability Insurance

Unlike other third-party professional liability policy coverage forms; Cyber Liability policy forms can include first-party coverage parts that pays for the immediate first-party breach response expenses, in addition to, loss of income resulting from network failures; extortion expenses as well as fines or penalties associated with regulatory actions.



Partnership

Most Cyber Liability insurers offer their policyholders a choice of breach response services, typically from a list of pre-approved vendors. Many allow the policyholders own choice of vendor.

Most insurers also grant policyholders access to a complimentary cyber risk management portal that includes the most updated information on emerging cyber threats and the latest reports on risk mitigation measures and practices.

Support Best Practices in Risk Management

- Cyber Expertise
- Understanding the Environment & Exposures
- Developing Solutions

Benchmarking

- Understand what peers are doing about risk transfer
- Information is in the rearview mirror
- Risk appetite
- Doesn't tell the whole story
- So....how do we use data and analytics to be more forward looking?

Science vs. Art

- Ever evolving environment
- Lack of data let underwriters to “guess” at the exposure
- Application process – more complete reporting of exposures. Questions are changing
- Adoption of 3rd party data – “credit score”
- NIST or ISO assessments
- Differentiator of industries
- Analytics can not model unknowns – GDPR, unknown threat vectors

What makes Good analytics?

- Predictive modeling that allows you to make decisions
 - Model includes current loss data
 - Large database
 - Predicts loss scenarios
 - Provides evaluation of retentions, limits and premiums
 - Allows variations in data input

Speakers

- **Frank Rivera**
 - Director, Risk Management & Workers' Compensation, Massachusetts Port Authority
- **Tamika Puckett**
 - Director, Office of Enterprise Risk Management, City of Atlanta – Department of Finance
- **Michael Phillips**
 - Cyber and Executive Risk, Beazley Group
- **Justin Yost**
 - Information Security Architect, Port of Portland
- **Sou Ford**
 - SVP, Atlantic/SE Cyber Team Leader, Willis Towers Watson, Atlanta, GA