



STRATEGIC
Leadership
FORUM
*The future of
payments today*



- **Security/protection of the payments systems**

- **Session 3, Segment 2**
- **Wednesday, October 14th, 2009**

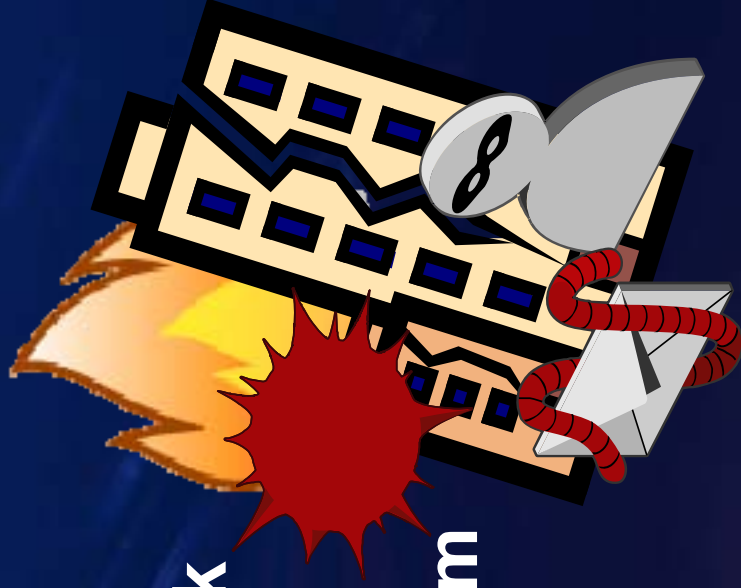
John Seddon



- President
- Deknatel Seddon & Associates

Agenda

- Risk factors and measuring risk
- Security of the payments system



Question: Are there any sources of risk data or “rules of thumb” available?

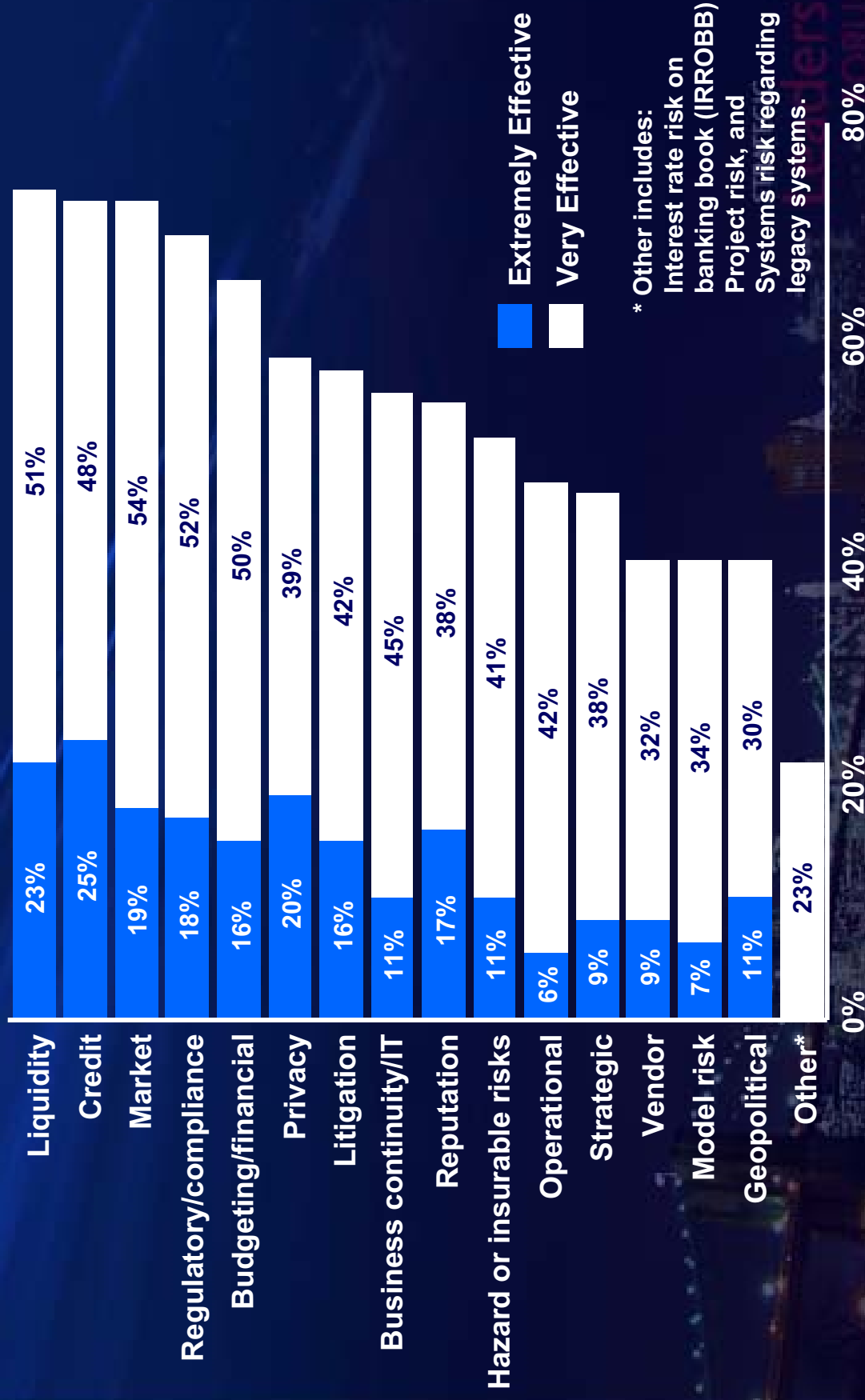
- There are some published data available (see slide 25).
 - This data is residual risk data – i.e. after controls have been implemented – and is specific and relevant only to the company which collected the data.
 - The applicability of such data to any company other than the one which collected the data is doubtful, because different companies implement different controls and achieve different levels of control effectiveness/risk reduction.
- We have not found publicly available, consistently collected, risk data suitable for developing, “rules of thumb” .
- We recommend that any company use its own risk data – including inherent risk, control effectiveness, and residual risk data (see slides 8 - 11) and develop its own, and more relevant, “rules of thumb”^{STRATEGIC}
- We recommend that companies use the framework and methodology presented here (see slides 15, 17, and 27) to collect such risk data.

Question: Going away from this session, what three things should the audience do when they get back to their office?

- Look at your data breach response plan. Check it for completeness. Check that it has been thoroughly tested (see slide 29).
- Start collecting, measuring *and using* your company's own risk data (see slide 28) to make informed risk management decisions (slide 14).
- Monitor industry publications and blogs for information about the emerging controls, e.g. data field or end-to-end encryption, tokenization:
 - Look for information about the vendor's claims and early adopters' experiences regarding the effectiveness of these controls in reducing risk.
 - Look for information about the total cost of these controls.

This information can be used by the “close followers” to make informed, risk-based, return-on-investment based, selection decisions.

There are plenty of risks out there

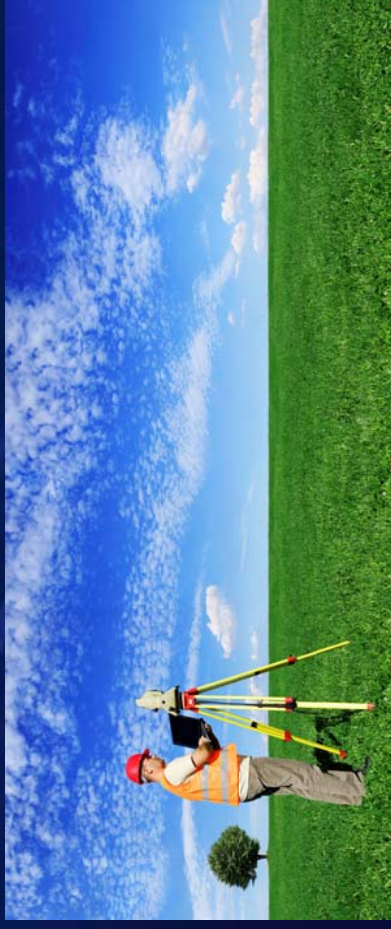


Source: Global Risk Management Survey, Deloitte, June 2009.

Five risk factors are involved in assessing risk and aligning the cost/risk model

Risk factors:

- Likelihood
- Impact
- Control effectiveness
- Residual risk
- Cost to implement control / reduce risk.



Likelihood and impact are primary factors in measuring risk

Likelihood

- Annualized rate of occurrence of the threat to the asset.
 - Measurement: Average annual probability(%)

Impact

- Magnitude of harm that could be caused by a threat / threat source's exercise of a vulnerability
 - Measurement: Average cost of incident (\$).

STRATEGIC

Leadership
FORUM

Source: NIST Risk Management Guide for Information Technology Systems, SP800-30, July 2002.

Annual Loss Expectancy

$$\text{Annual Loss Expectancy (ALE)} = \\ \text{Average annual probability (\%)} \\ \times \\ \text{Average cost of incident (\$)}$$

Risk measurement example:

- Average of 9 incidents per year (900%)
- Average of \$8,000 per incident
- Annual Loss Expectancy (ALE) = \$72,000^{TRATEGIC}

Source: NIST Risk Management Guide for Information Technology Systems, SP800-30, July 2002.

Inherent risk and residual risk can be used to align the cost/risk model

Residual risk

- Risk remaining after the implementation of controls

Inherent risk

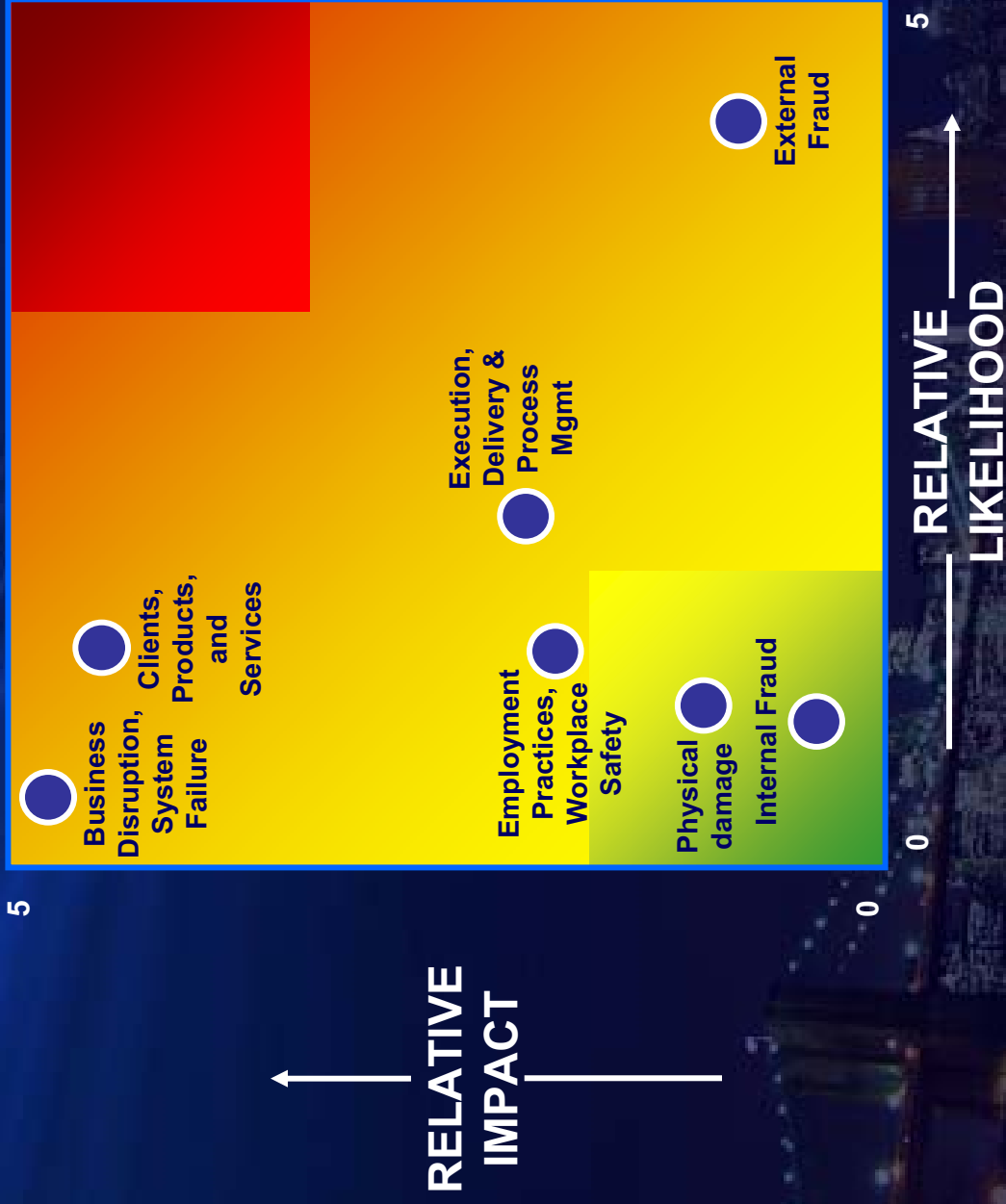
- Risk before the implementation of controls.

STRATEGIC

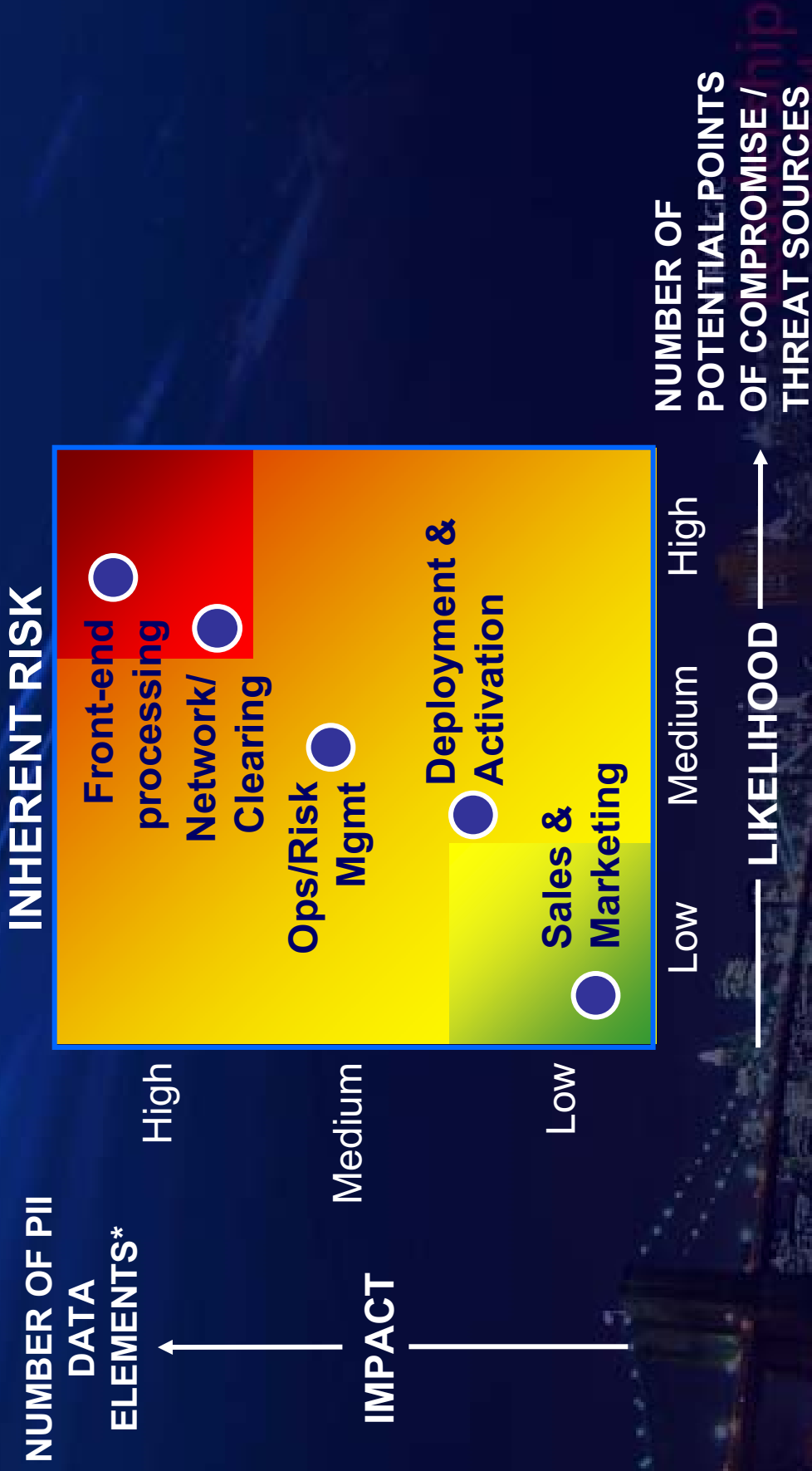
Leadership
FORUM

Source: NIST Risk Management Guide for Information Technology Systems, SP800-30, July 2002.

Residual operational risk for U.S. banks - based on loss data



Inherent data security risk for acquirer merchant processor



* Personally Identifiable Information. For definition, see Guide to Protecting Confidentiality of PII, National Institute of Standards and Technology, SP800-22, January 2009

Evaluate the cost of control versus risk reduction

Return On Control Investment =

Reduction in risk

Cost to implement and maintain control
(or “risk management option”*)

* Risk management options/decisions:

Respond (with controls, incident response plans)

Mitigate (e.g. with other controls)

Transfer (e.g. insurance, other third-parties)

Accept

STRATEGIC

Leadership
FORUM

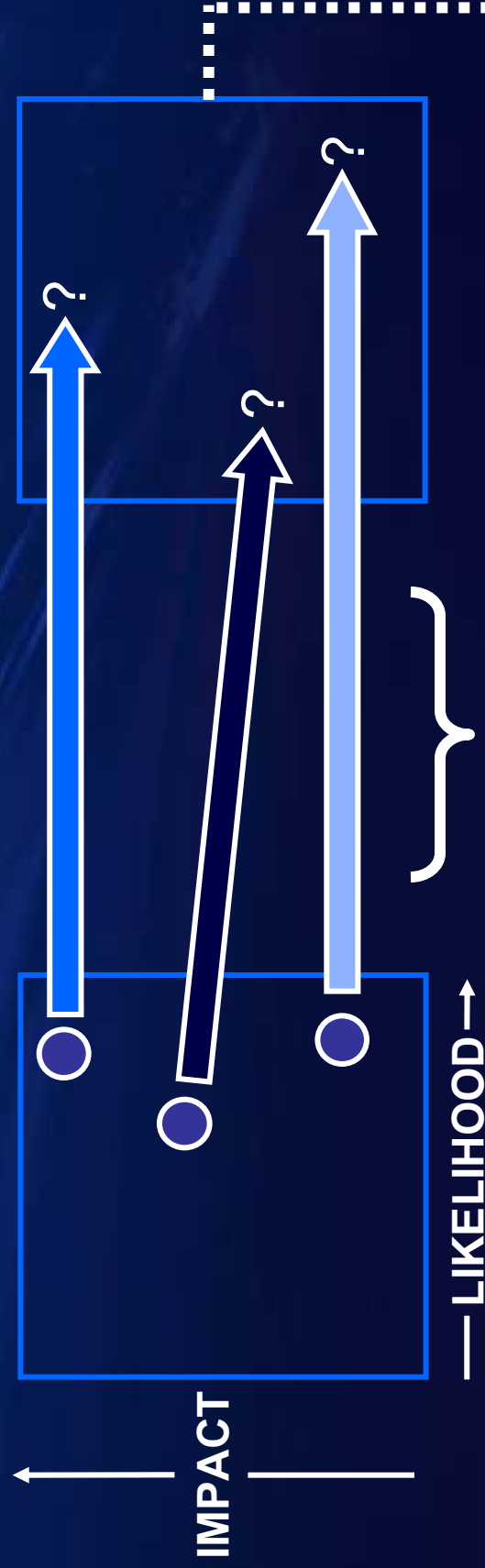
The future of
cybersecurity today

Four steps of risk assessment

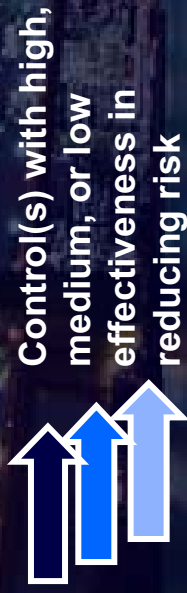
Step 1: Assess inherent risk

Step 2: Assess safeguards and controls

Step 3: Assess residual risk

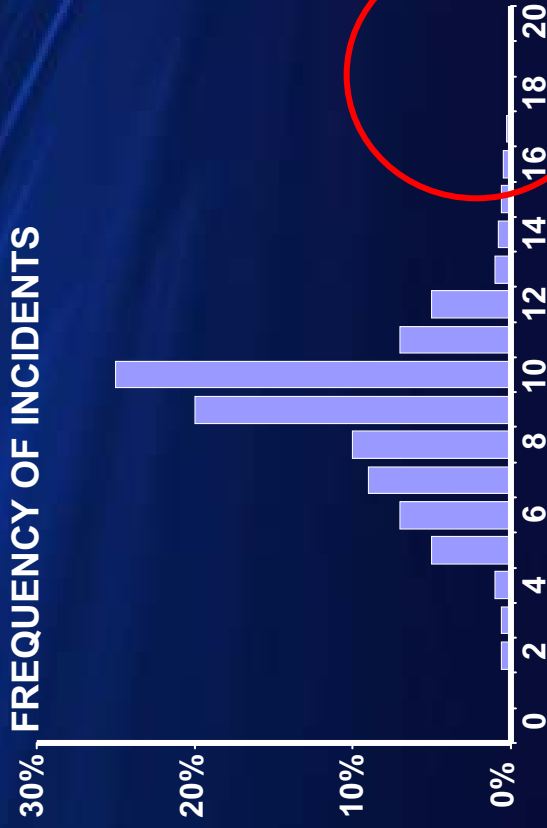


Step 4. Identify and prioritize areas for improvement

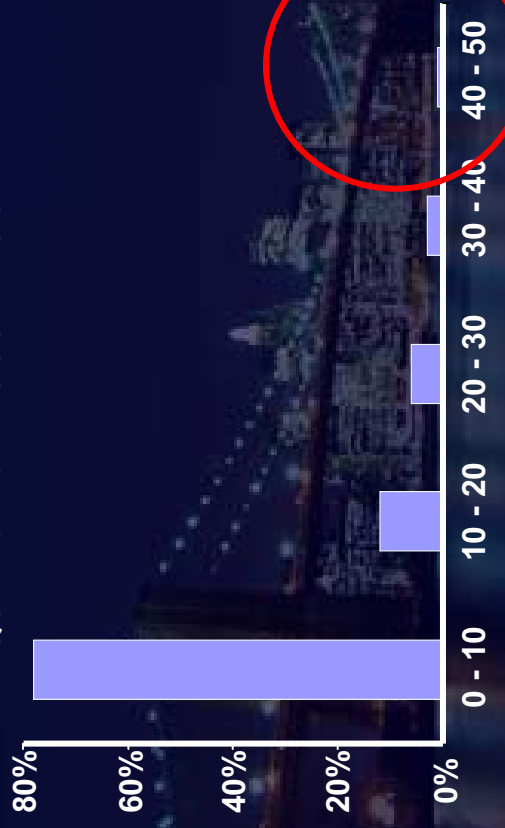


Evaluate distribution of incidents and loss amounts

FREQUENCY OF INCIDENTS

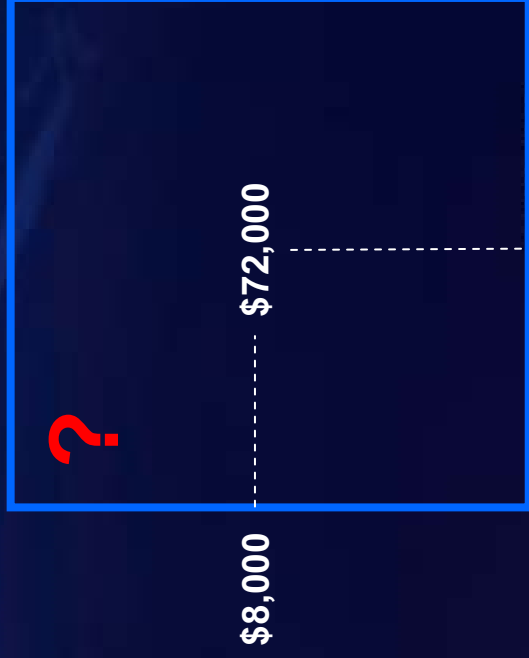


FREQUENCY OF LOSS AMOUNT



Example:

- Average of 9 incidents per year
- Average of \$8,000 per incident
- Annual Loss Expectancy (ALE) is \$72,000

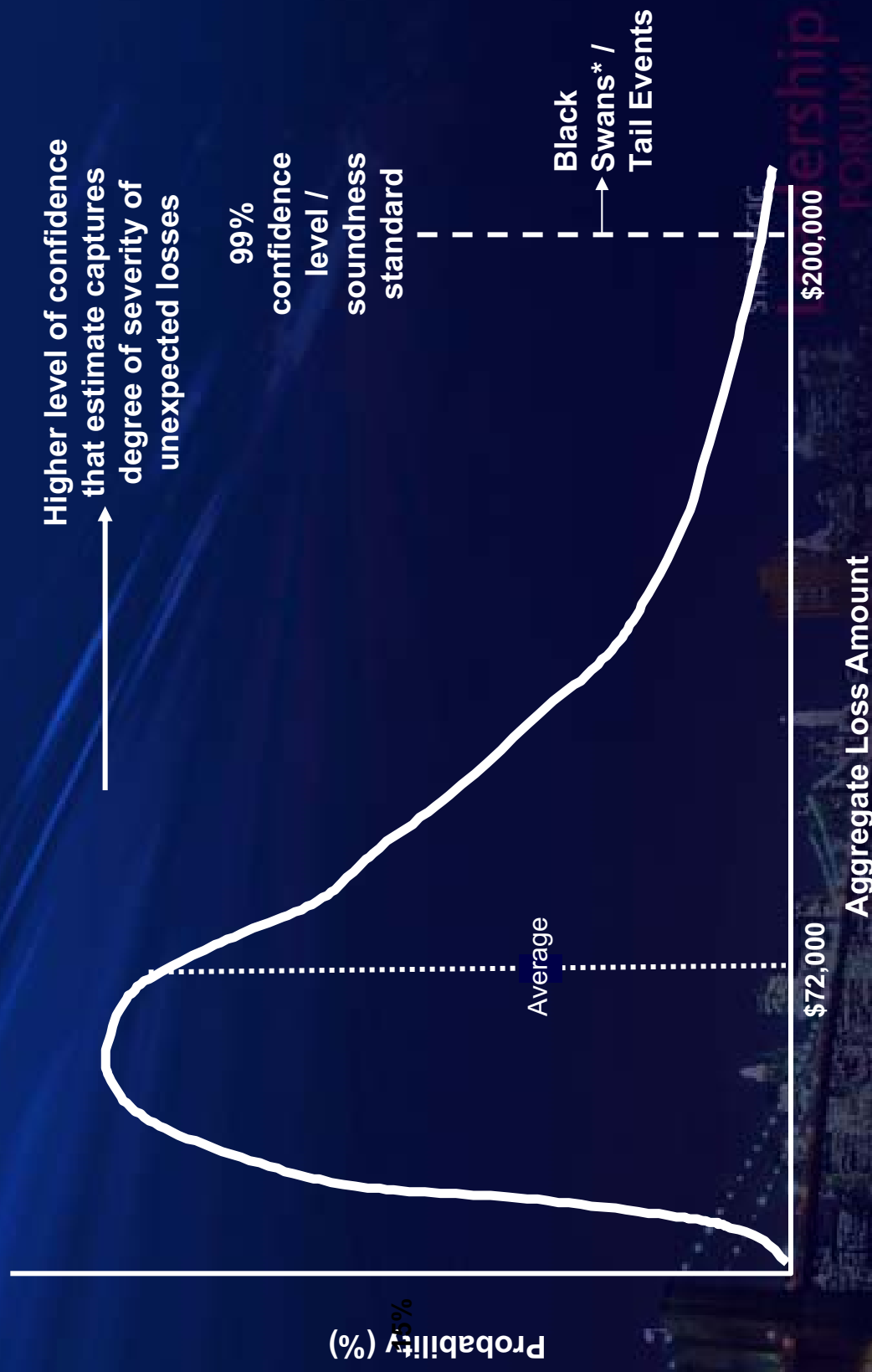


900%

Strategic Leadership FORUM

The future of payments today

Stochastic modeling provides a confidence level for exposure



* The Black Swan: The Impact of the Highly Improbable, by Nassim Nicholas Taleb, 2007

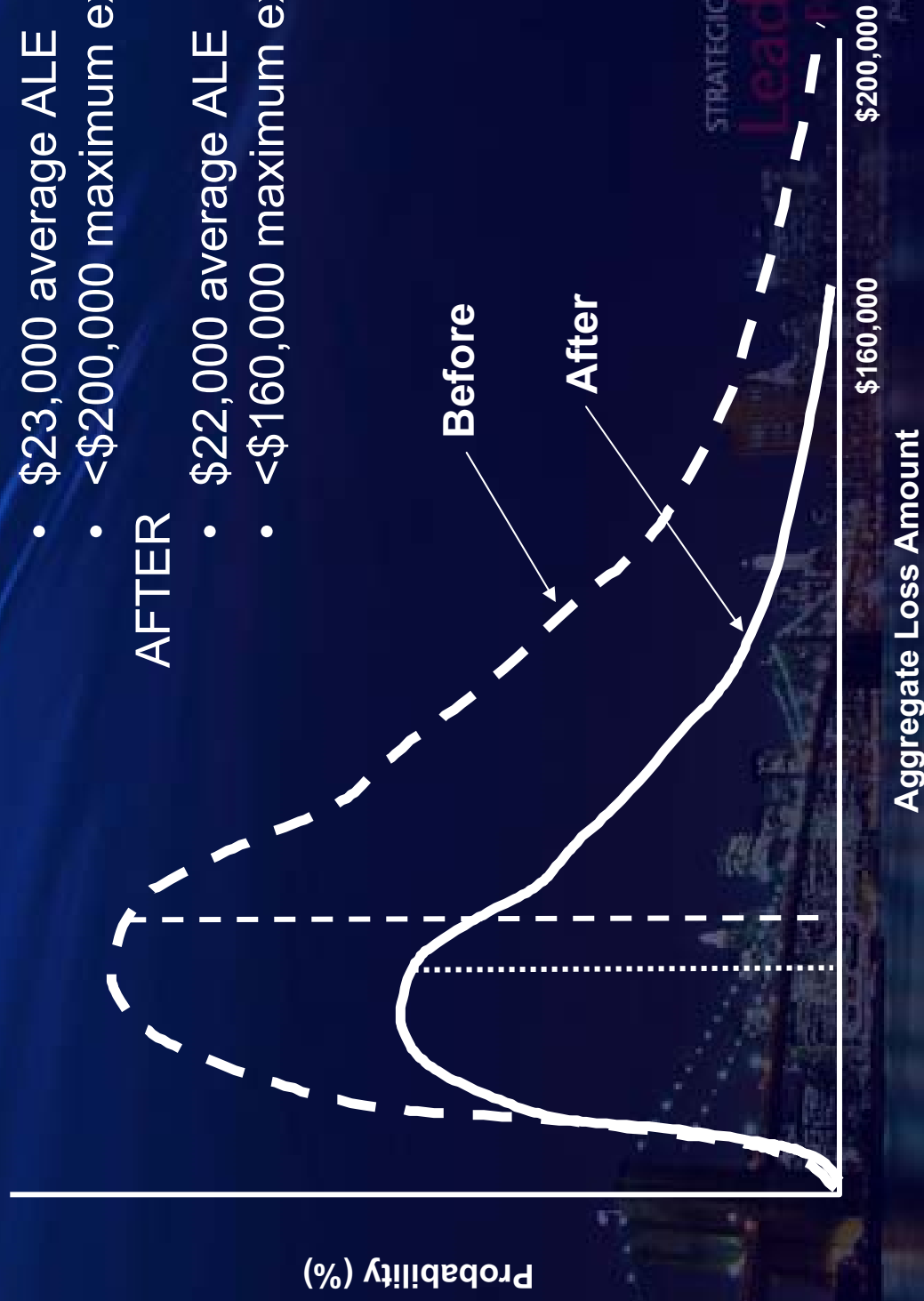
Whichever measure you use - the goal is to manage risk - “measure to manage”

BEFORE:

- \$23,000 average ALE
- <\$200,000 maximum exposure

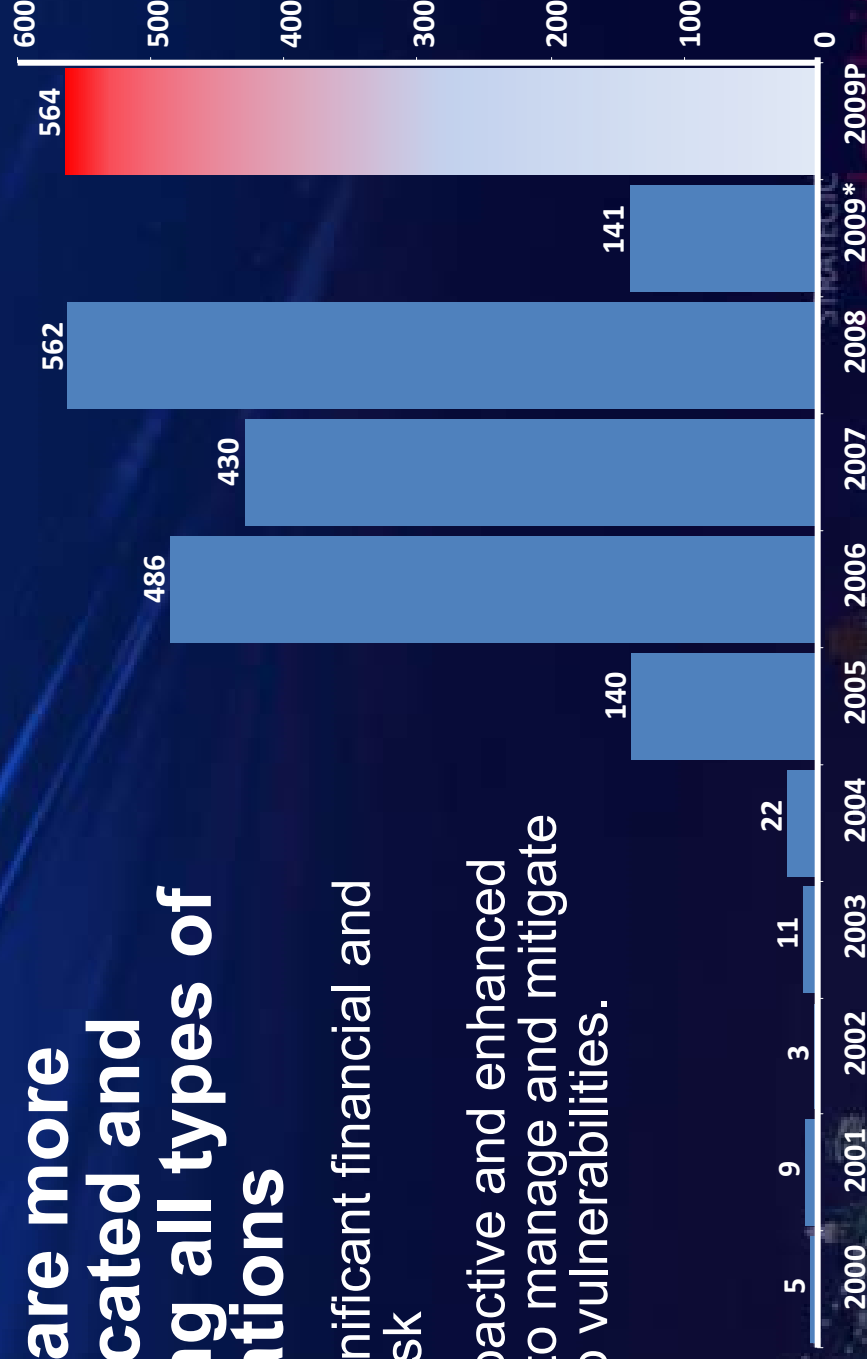
AFTER

- \$22,000 average ALE
- <\$160,000 maximum exposure



The payments systems are always under attack

- **Attacks are more sophisticated and impacting all types of organizations**
 - Present significant financial and structural risk
 - Require proactive and enhanced processes to manage and mitigate exposure to vulnerabilities.



* Reported through April 3, 2009, 2009P = Projected
Source: //datalossdb.org/statistics

We need to respond with organization-wide, multi-dimensional initiatives

- Pro-active and ongoing management of customer data
- Augmentation of efforts to actively meet network and/or regulatory compliance
- Good practices - beyond controls compliance
- Monitoring and forecasting
- Across all areas of the organization.

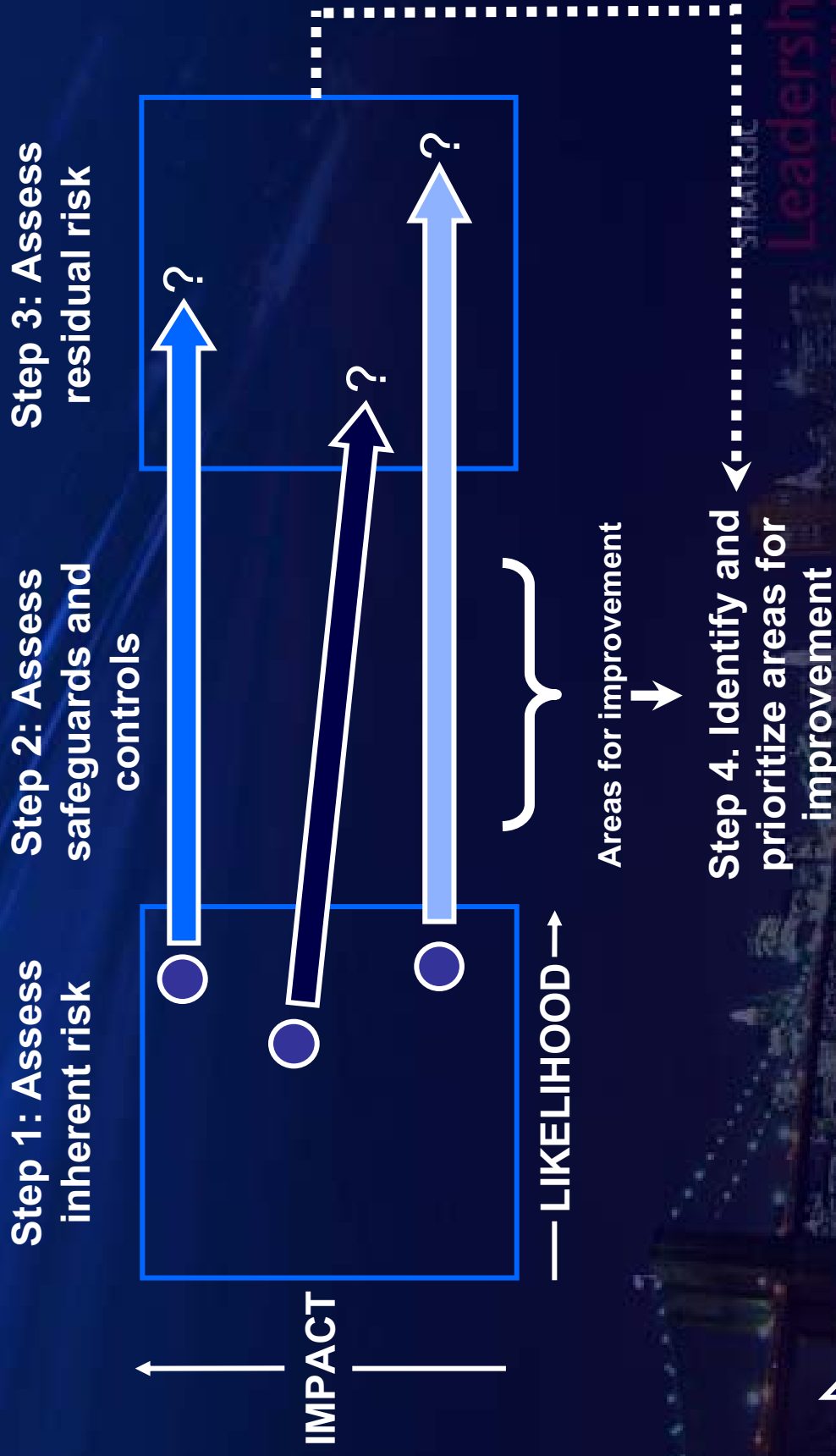


STRATEGIC

Leadership
FORUM

The future of
payments today

The four steps can be applied to assess data security risk



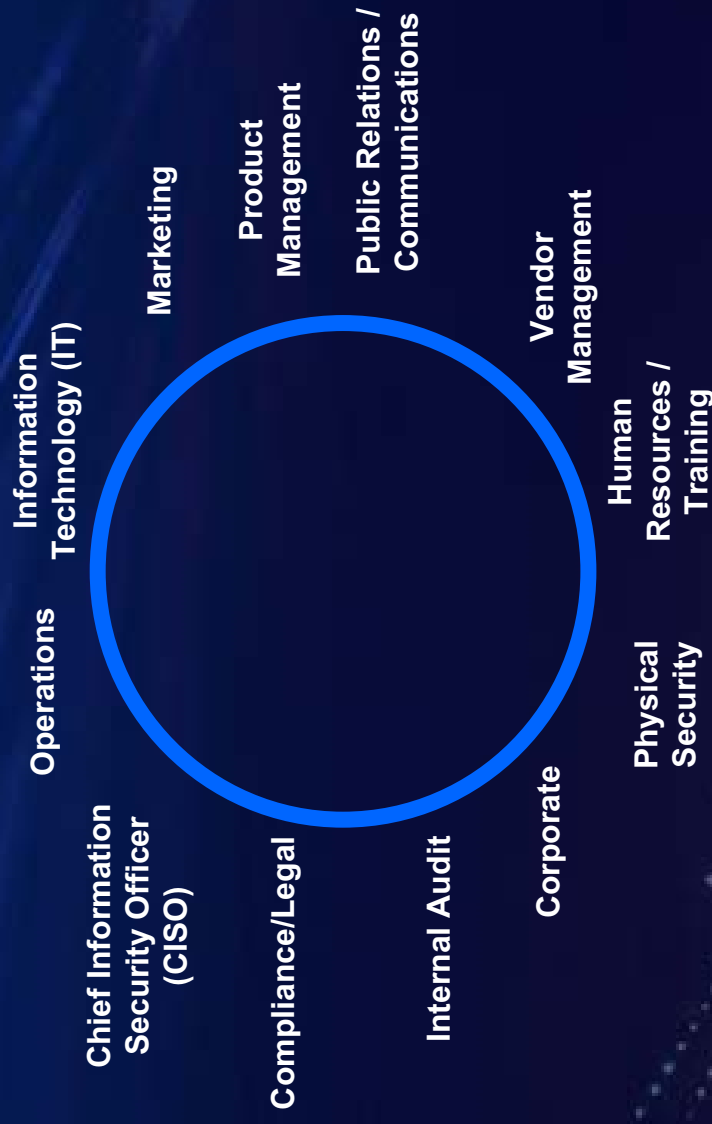
Control(s) with high, medium, or low effectiveness in reducing risk

Step 1 considers all vulnerabilities for assets at risk

- **Assets**
- **Data**
 - Electronic and hard copy data,
 - Data stored, processed, and in transit
- **Brand**
- **Reputation**
- **Personnel**
- **Across the value chain:**
- **Merchants and businesses**
- **Acquirer processors and third parties**
- **Banks, financial intermediaries and payment networks**

....and involvement of all the relevant stakeholders

Any of these areas could be handling assets at risk....



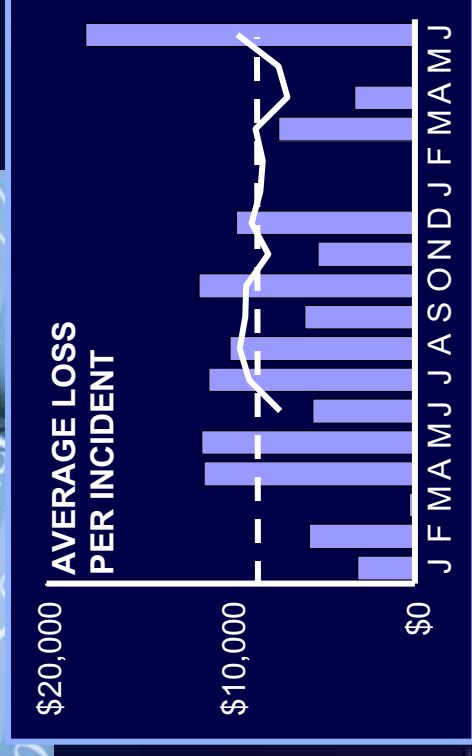
....they may also present weaknesses in controls and response plans.

STRATEGIC
Leadership

Consult internal and external sources for risk data

Internal

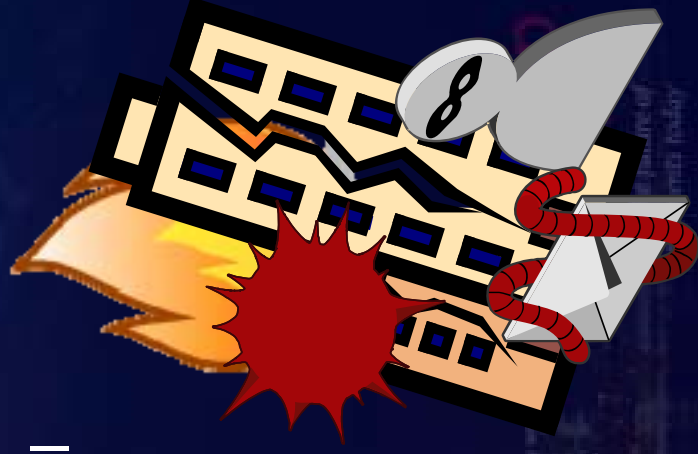
- Actual loss data
- Near misses
- Red flags
- Investigation reports
- Audit and examiner reports



Consult internal and external sources for risk data continued

External

- Open databases, e.g., Datalossdb, PrivacyRights.org
- Federal and state agencies, e.g.
 - Federal Bureau of Investigation,
 - Department of Justice,
 - New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC),
 - National Technical Information Service,
 - National Institute of Standards and Technology (NIST),
 - Department of Homeland Security,
 - California Office of Information Security (OIS)
- Payments and professional associations



Refer to, but do not limit to, published safeguards and controls guidance in Step 2

- Payment Card Industry (PCI)
 - Data Security Standard (DSS)
- National ACH Association (NACHA)
 - ACH Rules
- Federal Financial Institution Examination Council (FFIEC)
 - Wholesale Payment Systems
 - Retail Payment Systems
 - Information Security.



Build business cases for improvements in Step 4

- Calculate return on investment to prioritize initiatives

Area/Asset at Risk	Before			Cost Before			After			Cost After		Benefit = (4) - (8)
	Units Involved (1)	Value/Cost per unit (2)	Prob. of Event (3)	(1) * (2) * (3) = (4)	Units Involved (5)	Value/Cost per unit (6)	Prob. of Event (7)	(5) * (6) * (7) = (8)				
DIRECT												
Customer Notification (Certified Mail)	250,000	\$37,500	5%	\$37,500	187,500	\$3.50	5%	\$32,813	\$	54,688		
Reissued Cards	50,000	\$2,250	5%	\$2,250	37,500	\$2.25	5%	2,344	\$	3,906		
Fraud Account Monitoring	160,000	\$14,950	5%	\$239,200	120,000	\$14.95	5%	89,700	\$	149,500		
State/Federal fines or fees	250,000	\$5,000	5%	\$125,000	187,500	\$5.00	5%	46,875	\$	78,125		
PR and Media Management	1	\$25,000	1	\$2,500	1	\$15,000	5%	750	\$	1,750		
Forensic Investigation	1	\$25,000	1	\$2,500	1	\$15,000	5%	750	\$	1,750		
Attorney's Fees	350	\$500	1	\$17,500	200	\$500	5%	5,000	\$	12,500		
etc.												
INDIRECT												
Brand Reputation	1	\$1,000,000	10%	\$100,000	1	\$1,000,000	5%	50,000	\$	50,000		
Loss of Sales	1,000,000	\$70	10%	\$70,000,000	750,000	\$70	5%	2,625,000	\$	4,375,000		
etc.												
TOTALS AND COSTS												
Total Cost/Benefit								\$ 2,853,231	\$	4,727,219		
Implementation Cost				\$ 7,580,450	1	\$300,000	100%	300,000	\$	(300,000)		
Hardware and Annual Maintenance Support	1	\$0	100%	\$0	1	\$100,000	100%	100,000	\$	(100,000)		
Total Net Benefit of Implementation										\$ 4,327,219		



Total project ROI over 3 years for Direct Benefits only = 125%

Survival is today's reward for managing risk

- Start measuring likelihood and severity
- Apply basic averaging techniques
- Look at highest inherent risk area in more detail, for:
 - Distribution of incidents and severity
 - Cycles and periodicity
 - Tail events
 - Learn from other people's mistakes

Survival is today's reward for managing risk continued

- Take steps to reduce risk
 - Reduce severity (e.g., readiness, insurance)
 - Reduce likelihood (e.g., monitoring controls)
 - Reduce likelihood and severity (e.g., authorization levels)
 - Remember to update reporting
- Reassess
 - Different behavior/distribution of incidents after risk mitigation steps have been implemented.

Thank you

John Seddon
President
Deknatel Seddon & Associates
john@dekseddon.com