Will They EVER "Get" Security?

Jack Jones
CXOWARE

Session ID: PROF-M02
Session Classification: General Interest

News Flash...

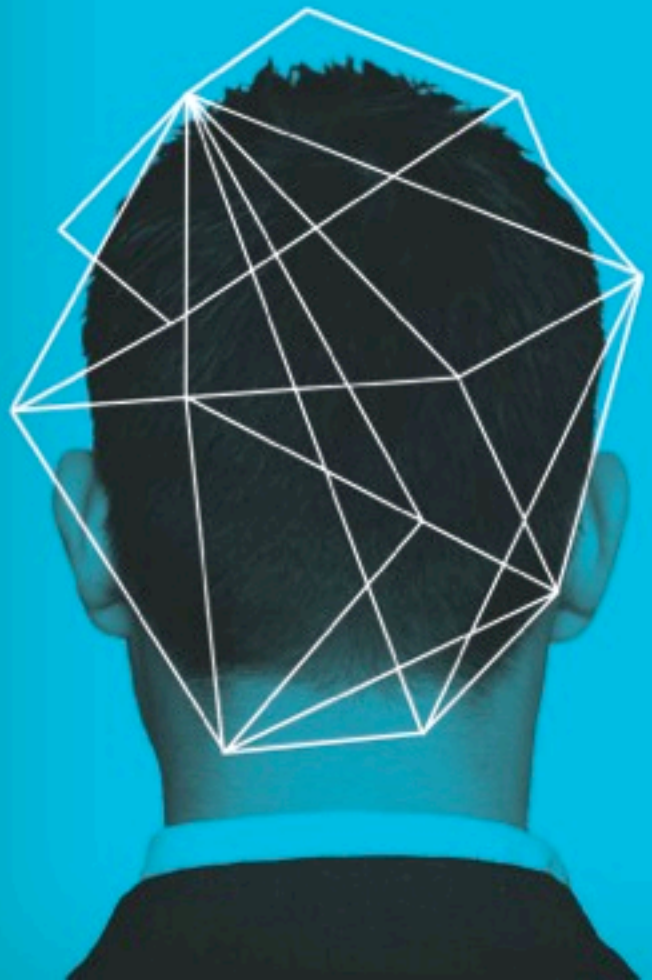
Management doesn't care about security

Question...

How are 1/4” drill bits similar to security?

What we'll cover...

- Infosec's value proposition
- Crippling misconceptions
- Packaging and conveying our value prop
- Be careful what you wish for...
- Q&A



Infosec's Value Proposition

Remember my question...

How are 1/4” drill bits similar to security?

Infosec's Value Proposition

Its affect on the frequency and magnitude of loss (i.e., managing risk)

Which is likely to be more meaningful?

We need to implement security technology/process/policy X because it's best practice

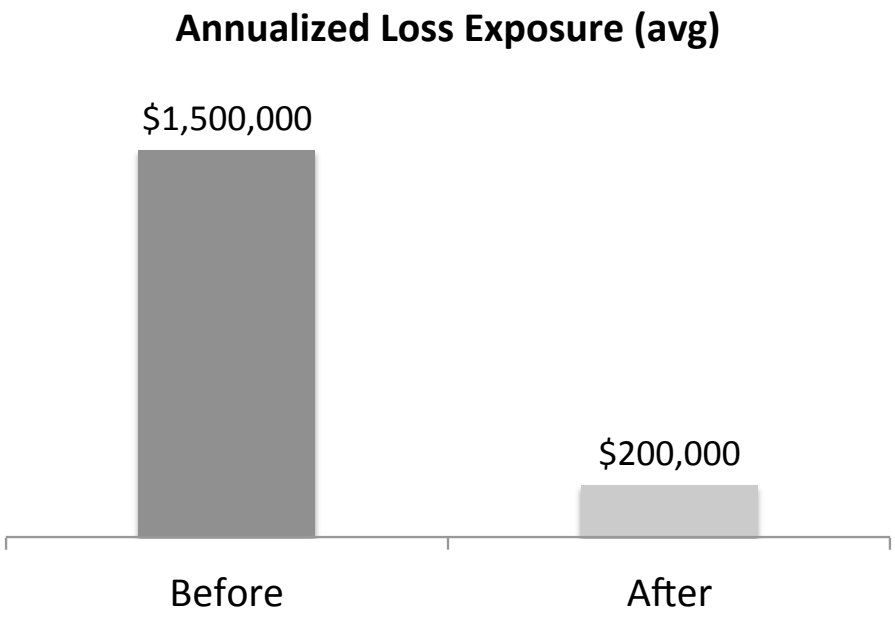
or...

If we implement security technology/process/policy X it will take us from a level 4 (high) risk to a level 2 (medium) risk

or...

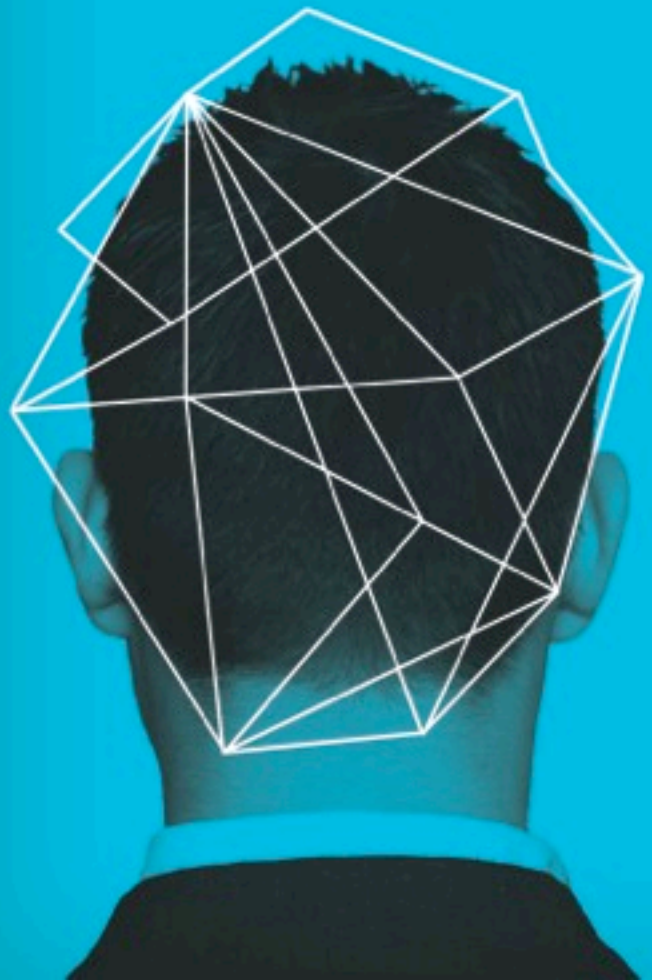
Which is likely to be more meaningful?

If we implement security technology/process/policy X at a cost of $120k, we'll reduce our average annualized loss exposure from $1.5M to $200k



News flash...

Management cares about exposure to loss



Crippling Misconceptions

Crippling misconceptions

- Risk can't be measured
- There isn't enough data for quantitative analysis
- Quantitative analysis is impractical
- Infosec risk is different from other forms of risk
- Business people will always accept risk
- You can do meaningful math on ordinal values

Risk ~~can't~~ can be measured

...but first you have to define it and understand it

- From a practical perspective, risk boils down to "exposure to loss"
- If you can estimate/measure the probable frequency of a loss event and the probable impact of that event, then you are measuring the risk associated with the event

A common problem though...

Recently reviewed an organization's risk register and found things like:

- Failure to patch vulnerabilities
- Default passwords
- Failure to make system backups
- Disgruntled employees
- Unencrypted laptops

Problem: These aren't loss events, so you can't assign a meaningful frequency and magnitude of loss to them

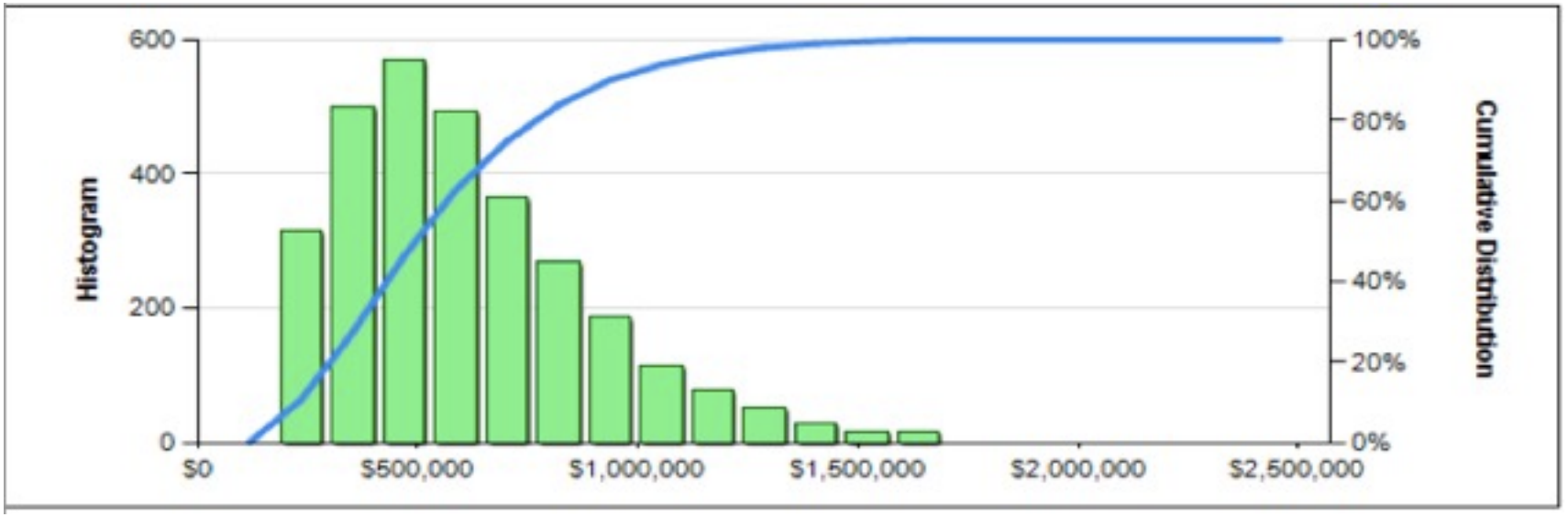
There is~~n't~~ enough data

- You have more data than you think you do, and you need less data than you think you do
  - You just have to know where to look and how to make the best use of what you have
  - Book: How to Measure Anything – by Douglas Hubbard
- Leverage ranges, distributions, and Monte Carlo

There is~~n't~~ enough data

Annualized Loss Exposure:

	Minimum	Average	Mode	Maximum
Primary				
Loss Events / Year	0.11	0.30	0.36	0.49
Loss Magnitude	$102,000	$1,500,000	$680,000	$4,900,000
Secondary				
Loss Events / Year	0.01	0.03	0.02	0.06
Loss Magnitude	$10,600	$3,600,000	$318,000	$29,000,000
Total Loss Exposure	$36,600	$546,023	$360,000	$1,500,000



Quantitative analysis is ~~im~~practical

- Quantitative analysis does NOT have to require a lot of research and data
  - Quick and dirty is often good enough
  - A lot of data is reusable across similar scenarios
- Effective use of ranges and distribution can faithfully represent the quality of your data

Infosec risk is NO different than other forms of risk

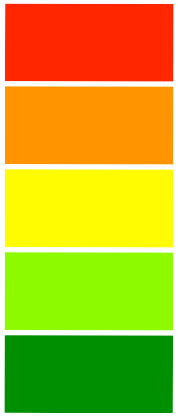
- Boiled down, risk is simple “exposure to loss”
- Exposure to loss is fundamentally the same in principle whether we’re dealing with armed conflict, personal injury, investments, or data breaches

Business people will NOT always accept risk

- When presented with good quantitative analysis, I've found business leaders to be remarkably risk averse
- The key is that the information we provide them has to be rational and defensible

You ~~can~~ can't do math on ordinal values

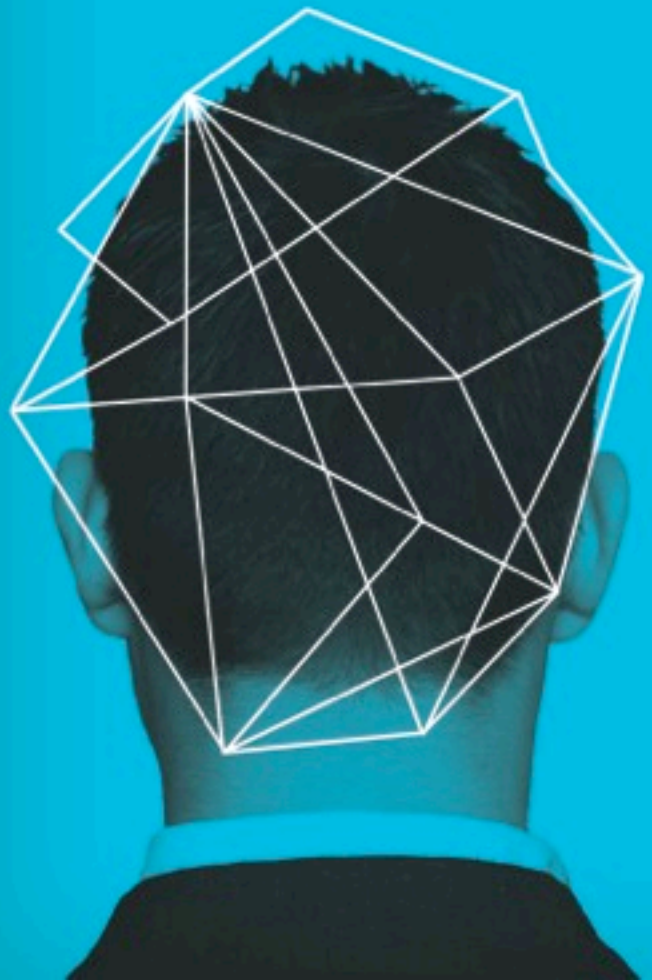
Qualitative Scale
(Ordinal)



Very High	5
High	4
Moderate	3
Low	2
Very Low	1

What does  x  equal?

What does +  equal?



Packaging and conveying our value proposition

What's the purpose?

- The purpose is to support well-informed decisions
- Understand what decisions are at stake and focus on providing only what's required to support those decisions
- This is also NOT about "convincing" executives to see things our way.

My criteria for communications:

- Clear – Simple terminology, no infosec/IT acronyms
- Concise – Less is more
- Accurate – Absent bias and hyperbole
- Useful – Meaningful and actionable

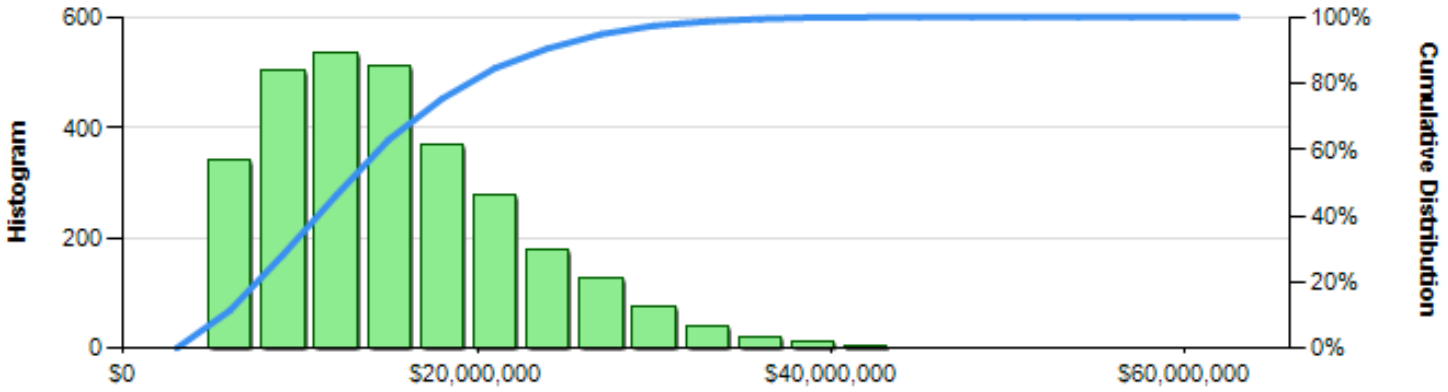
Keys to packaging and communicating

Above all, be able to defend what you present

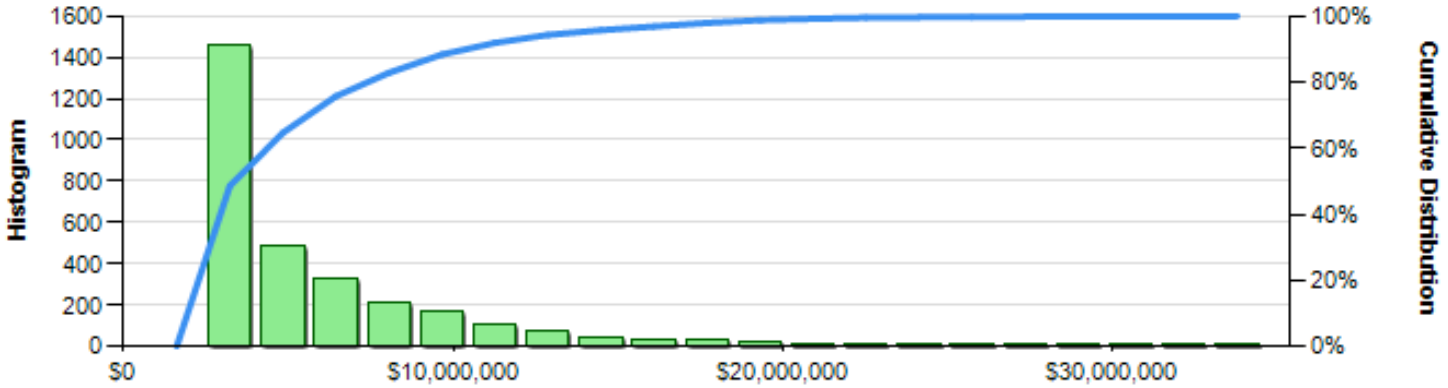
Examples...

Spending decision example

Current State: Before additional controls

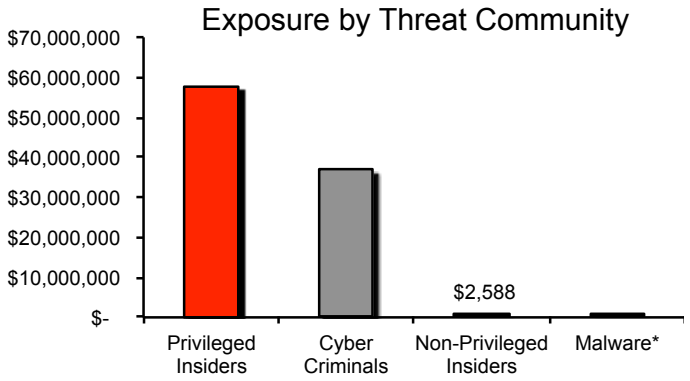


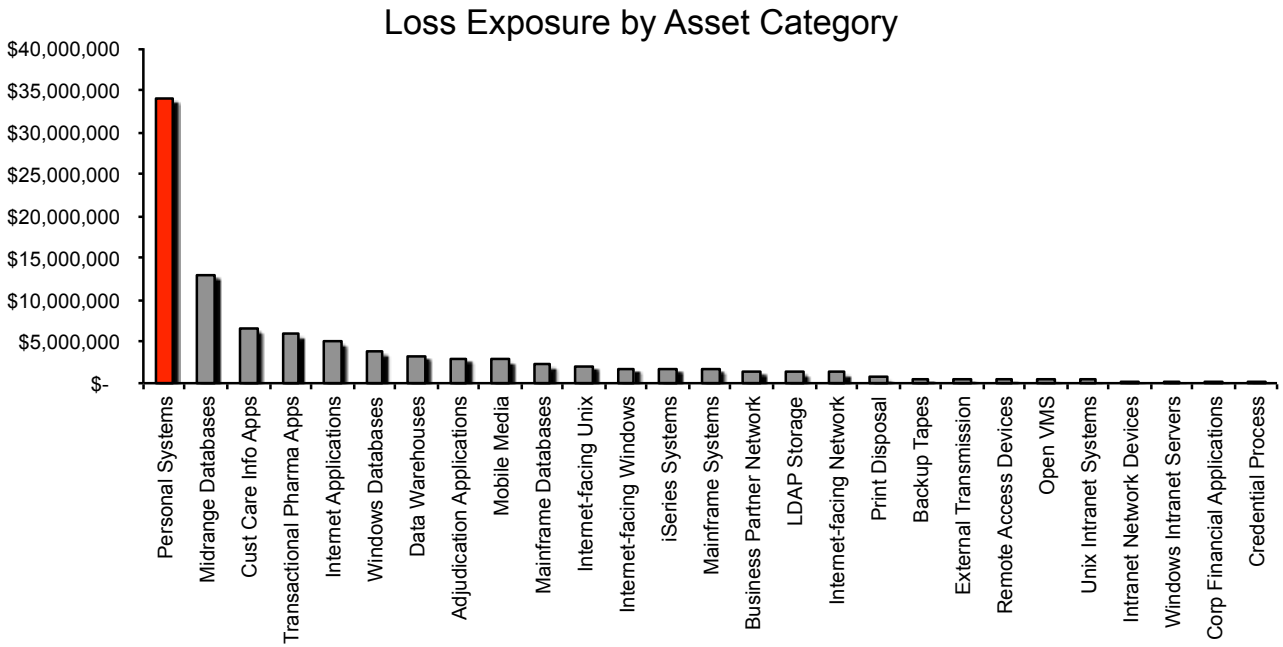
Future State: After additional controls



Prioritization example

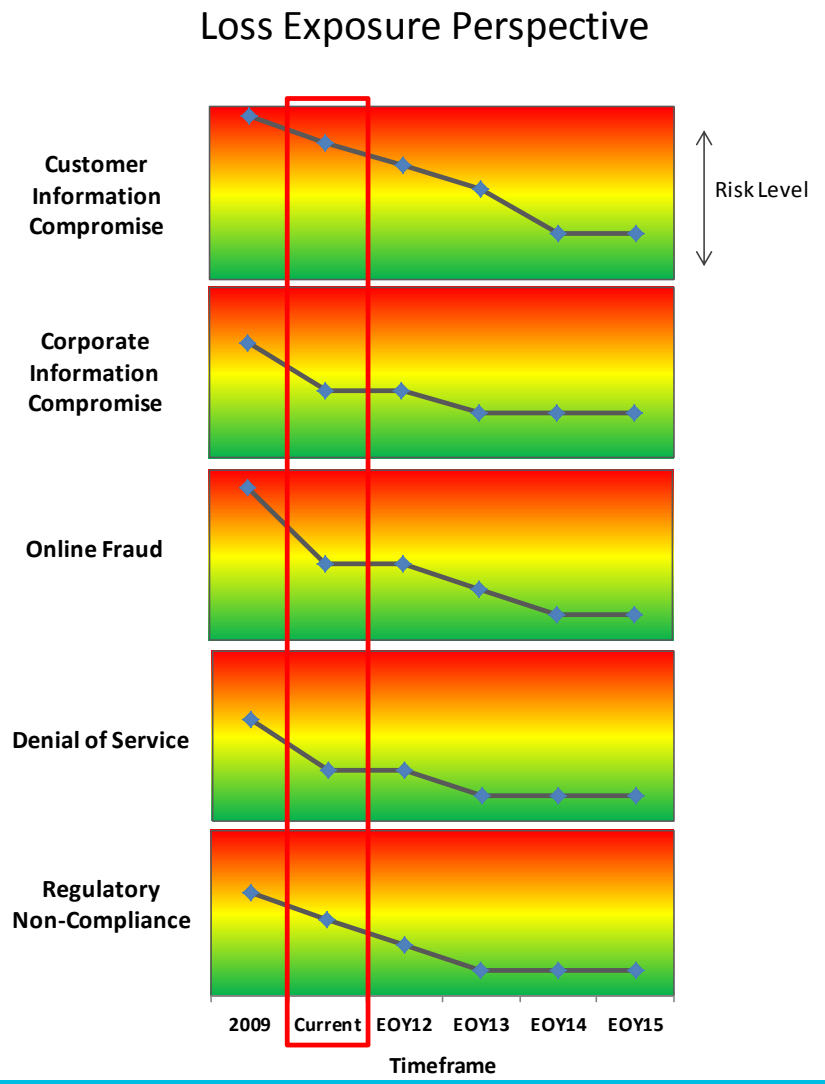
The most recent enterprise risk assessment found that insiders represent the most significant threat community (by 35% over cyber criminals), and that personal systems (desktops & laptops) represent the most significant point of exposure.





Multi-year strategy example

- Improved workstation protection and malware controls account for the significant reduction in loss exposure between 2009 and 2013.
- Data leakage controls, combined with workstation and malware controls mentioned above have driven the reduction in loss exposure for sensitive corporate information.
- Implementation of advanced anti-fraud measures in 2010 and 2011 have significantly reduced the volume of online fraud losses.
- Denial of service exposure was reduced in 2010 thru an upgrade in the network architecture. Future loss exposure will be further reduced in 2013 with a change in Internet service providers.
- Regulatory requirements continue to stiffen, which has slowed progress in reducing this exposure. Plans for 2012 and 2013 should result in additional loss exposure reduction.



Loss Exposure

Total Loss Exposure					
Percentiles					
5%	25%	50%	75%	95%	Most Likely (Mode)

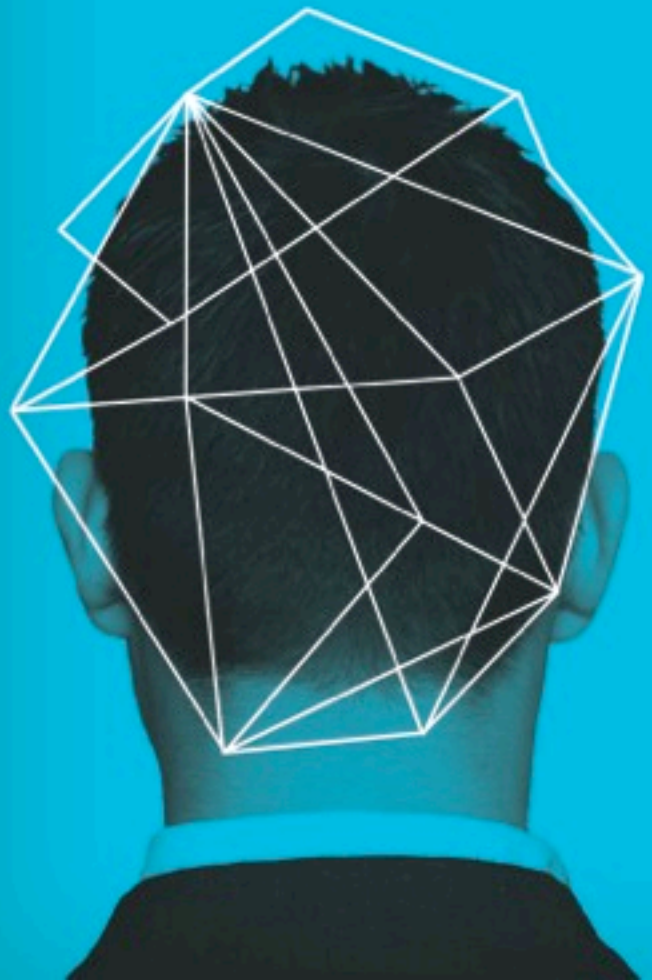
Risk Reduction Opportunities

Asset Group	Mitigation Component	Exposure Reduction
Internet Applications	Code Compliance	$33M
Personal Systems	Patch & Configuration Management	$27M
Internet-facing Windows Servers	Patch & Configuration Management	$5M
Data Warehouses	Access Privileges Management	$2M

Analysis identified four risk management opportunities that have the potential to reduce the organization's aggregate exposure by as much as $67M (~30% of the aggregate total).

Other suggestions:

- Match the form of your message to what your stakeholders are used to (PowerPoints? Text? Charts? Numbers? Colors?)
- Limit “eye candy”. The use of colors should be strategic and intentional. Don’t overdo it!



Be careful what you wish for...

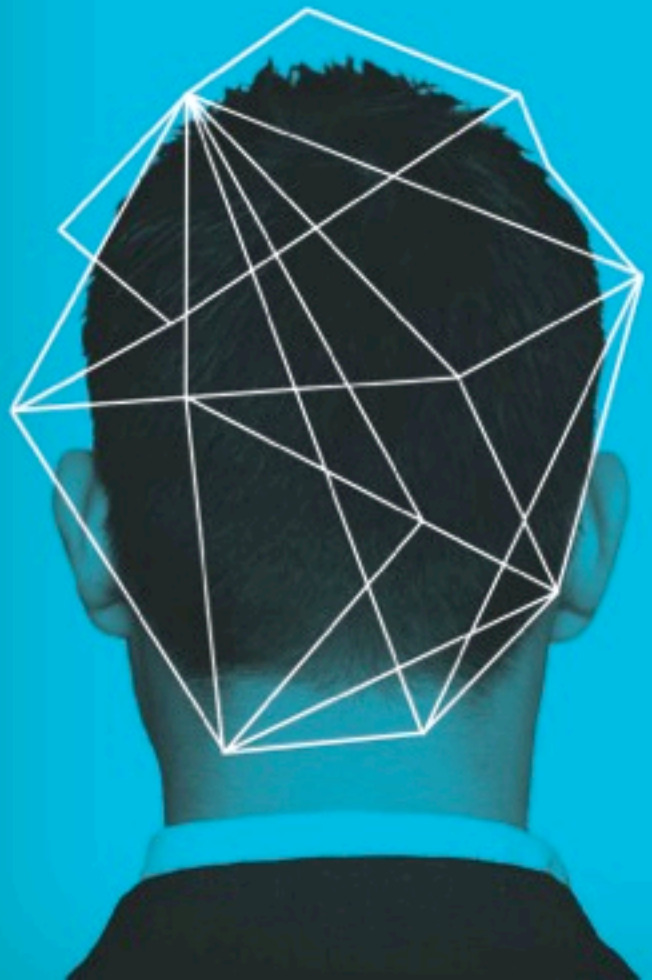
Be careful what you wish for...

So, you've demonstrated that you deserve a seat at the table.

Now what?

Things to be prepared for...

- A thirst for more...
- Politics (oh joy)
- Decisions you don't agree with



Wrapping up...

Summary

- Infosec's value proposition is its effect on the frequency and magnitude of loss. We're missing the target unless/ until we articulate it in those terms
- Misconceptions about risk and quantitative analysis seriously impede our ability to represent our value proposition effectively
- Effectively packaging and conveying our value proposition requires focus, clarity, brevity, and controlling our personal biases
- Successfully representing our value proposition can put us at the "big person table" – with all that entails

Resources

- How to Measure Anything – by Douglas Hubbard
- The Failure of Risk Management – by Douglas Hubbard
- Introduction to Factor Analysis of Information Risk (FAIR) – by Jack Jones
- Coming soon – a series of updated resources to help prepare for the The Open Group FAIR certification exam

Questions

For more information:

URL: www.cxoware.com
E-mail: info@CXOWARE.com
Phone: 866.936.0191