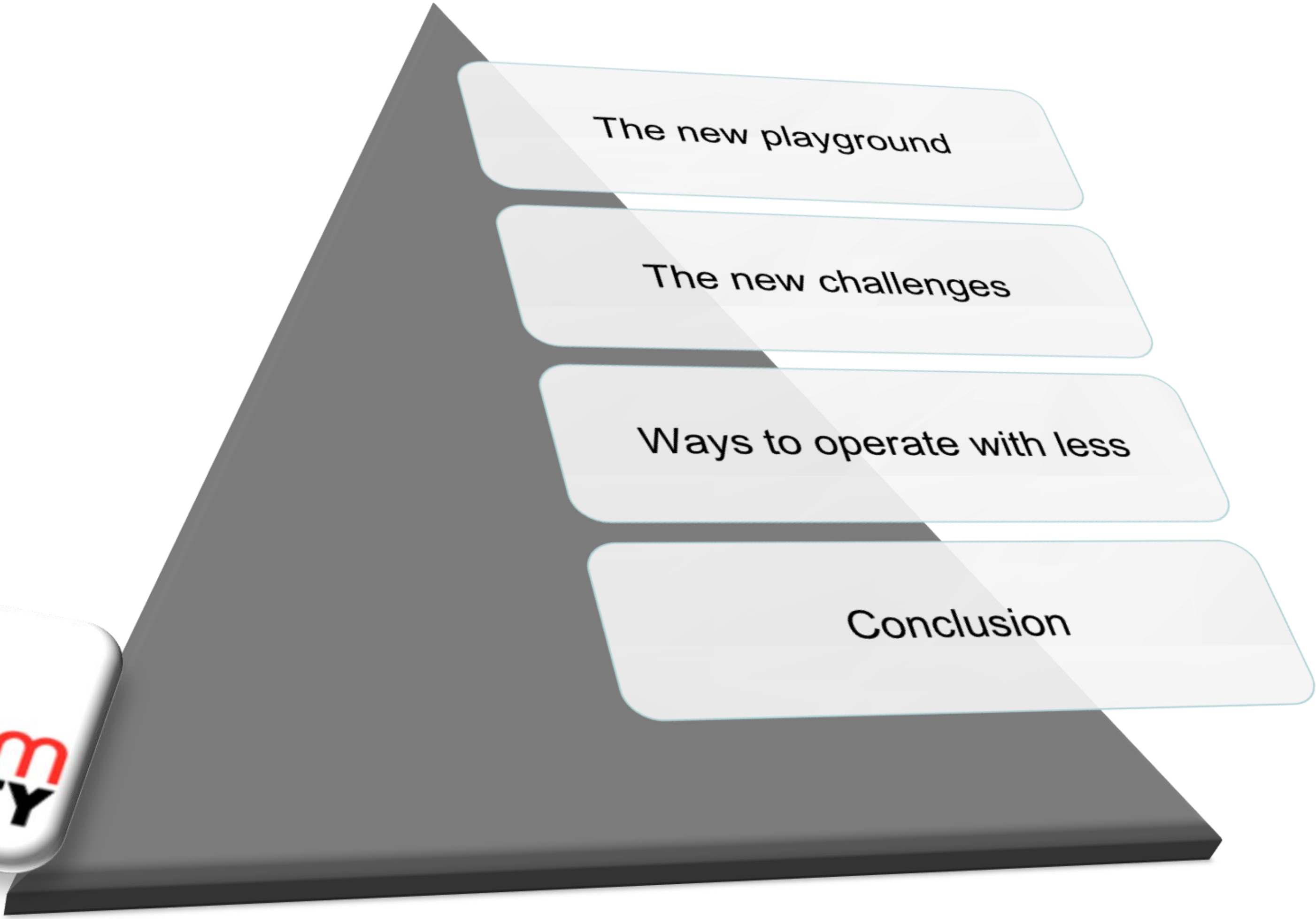
Ασφάλεια πληροφοριών Vs. Οικονομική ύφεση .... σημειώσατε 1

Notis Iliopoulos
Director of Technology
MSc InfoSec, MBIT, CISA, CISM, ISO27001LA



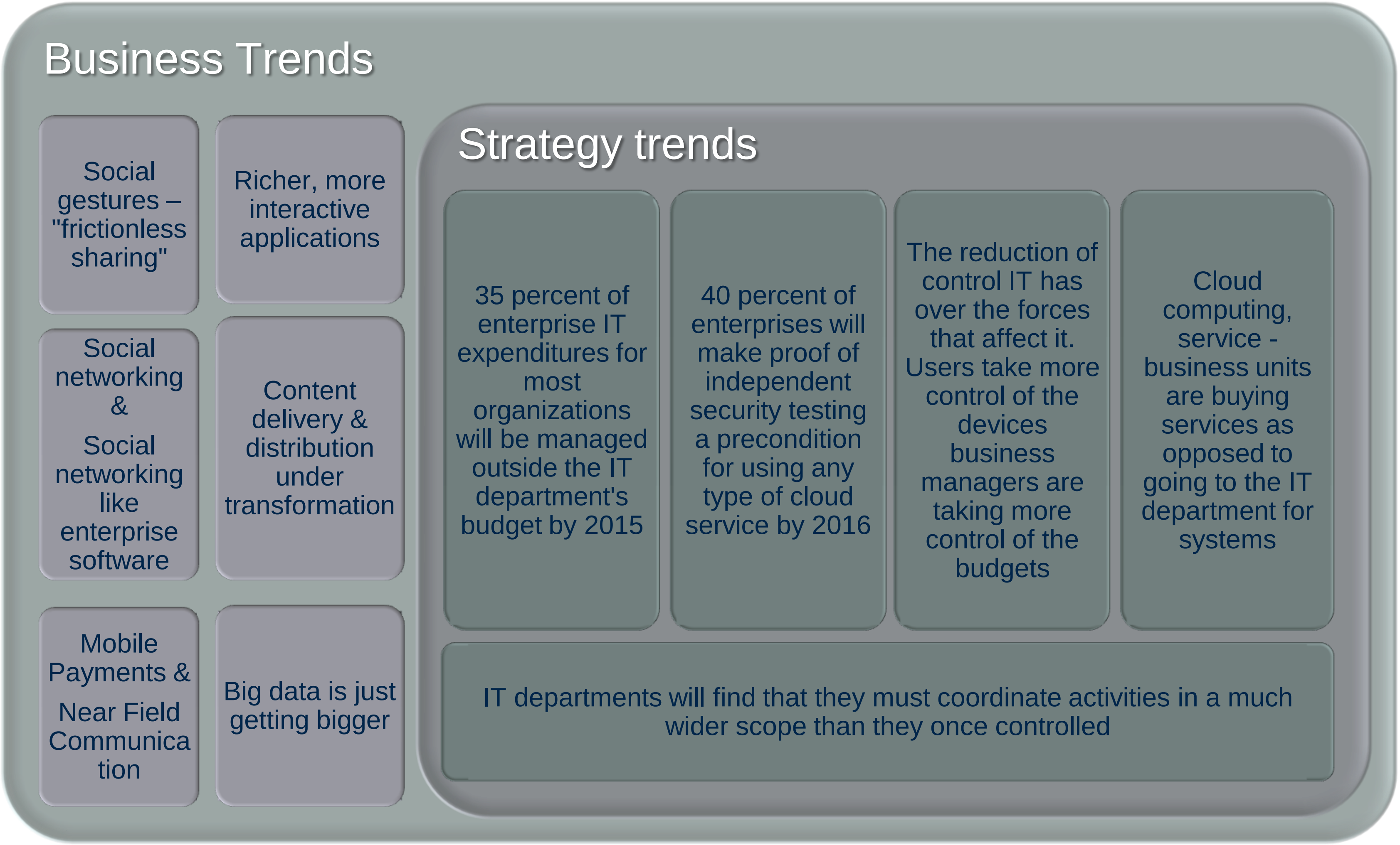
The new playground

The new challenges

Ways to operate with less

Conclusion

Setting the playground – the business perspective



Business Trends

Social gestures – "frictionless sharing"

Richer, more interactive applications

Social networking &

Social networking like enterprise software

Content delivery & distribution under transformation

Mobile Payments &

Near Field Communica tion

Big data is just getting bigger

Strategy trends

35 percent of enterprise IT expenditures for most organizations will be managed outside the IT department's budget by 2015

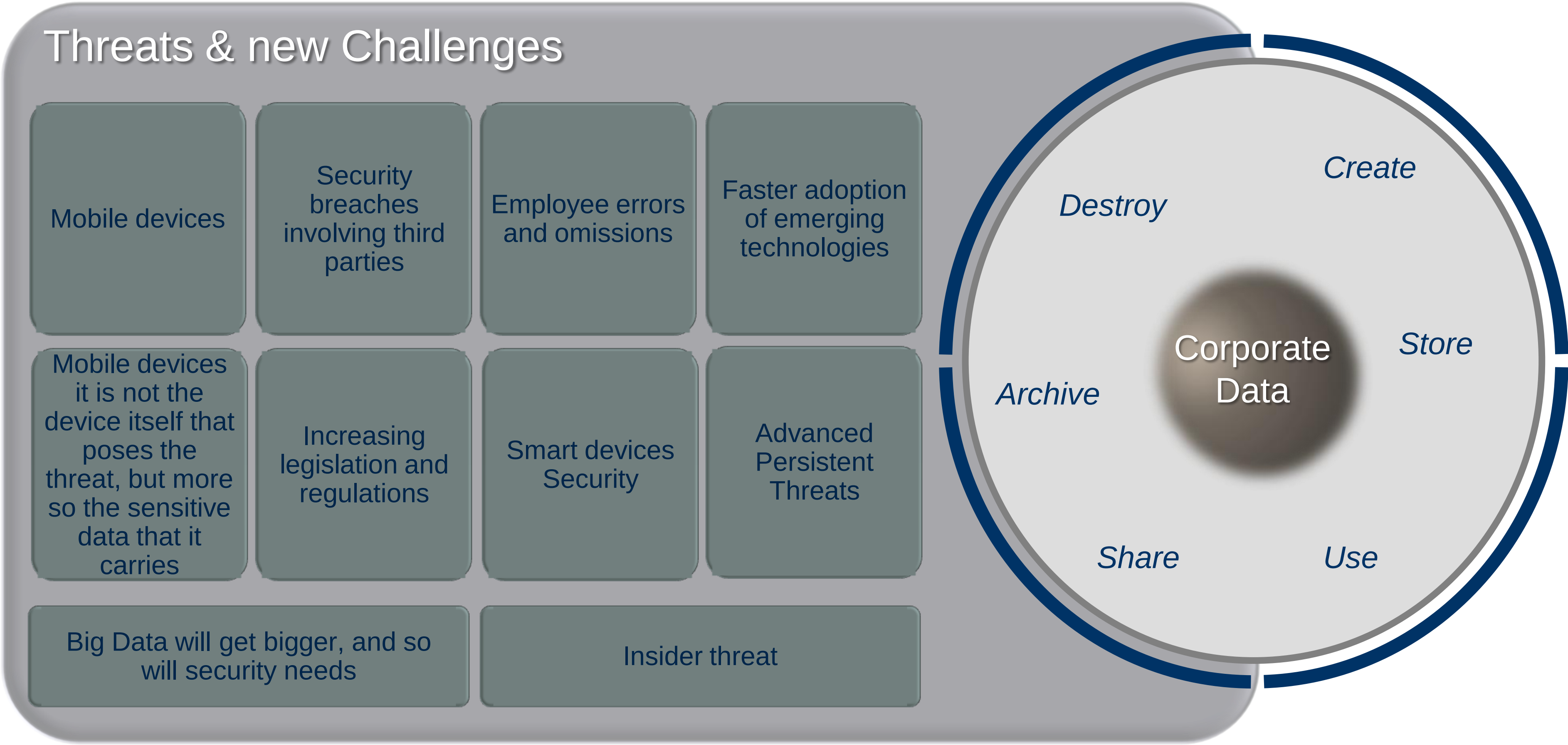
40 percent of enterprises will make proof of independent security testing a precondition for using any type of cloud service by 2016

The reduction of control IT has over the forces that affect it. Users take more control of the devices business managers are taking more control of the budgets

Cloud computing, service - business units are buying services as opposed to going to the IT department for systems

IT departments will find that they must coordinate activities in a much wider scope than they once controlled

Setting the playground – the risks & challenges



Threats & new Challenges

- Mobile devices
- Security breaches involving third parties
- Employee errors and omissions
- Faster adoption of emerging technologies
- Mobile devices it is not the device itself that poses the threat, but more so the sensitive data that it carries
- Increasing legislation and regulations
- Smart devices Security
- Advanced Persistent Threats
- Big Data will get bigger, and so will security needs
- Insider threat

Corporate Data

Create

Store

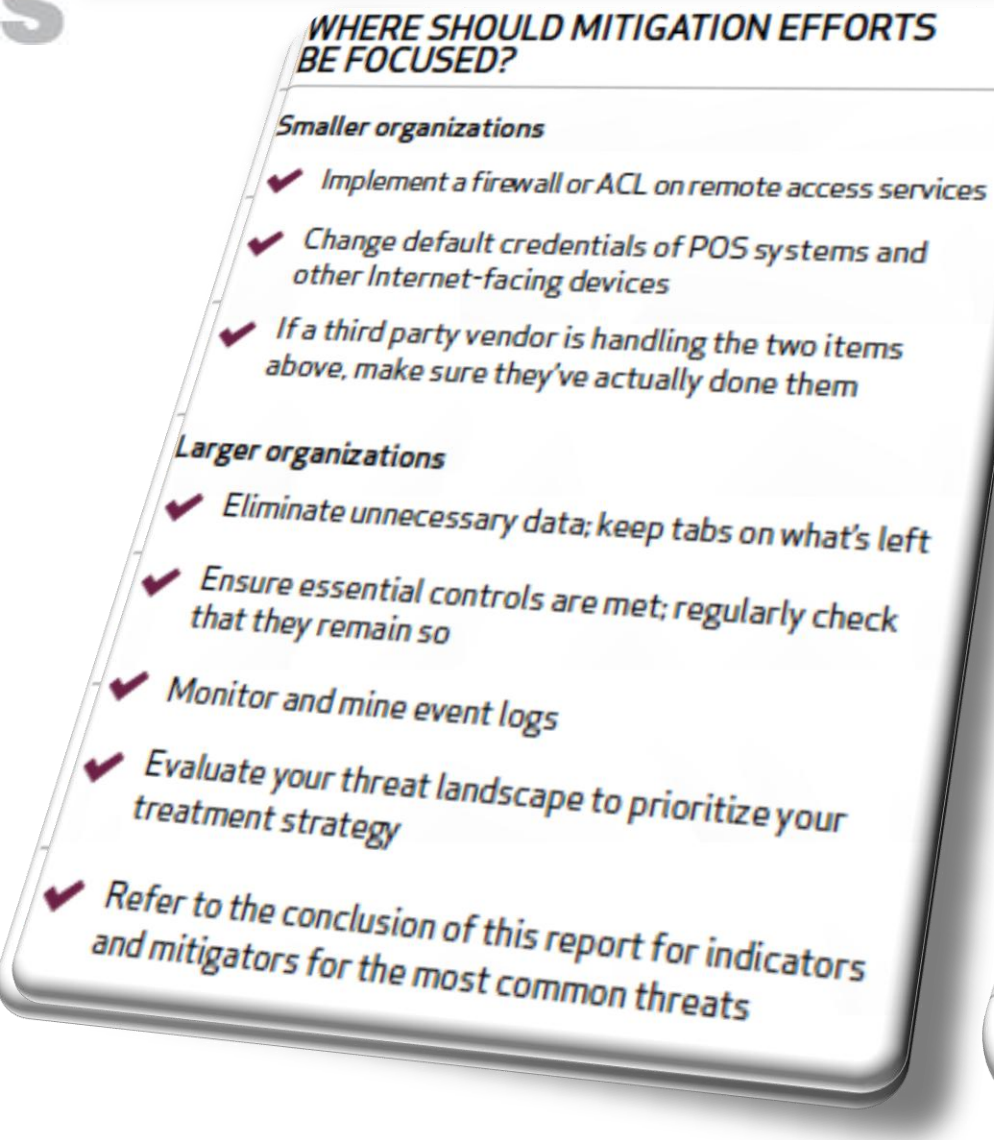
Use

Share

Archive

Destroy

Setting the playground – the risks & challenges



WHERE SHOULD MITIGATION EFFORTS BE FOCUSED?

Smaller organizations

✓ Implement a firewall or ACL on remote access services

✓ Change default credentials of POS systems and other Internet-facing devices

✓ If a third party vendor is handling the two items above, make sure they've actually done them

Larger organizations

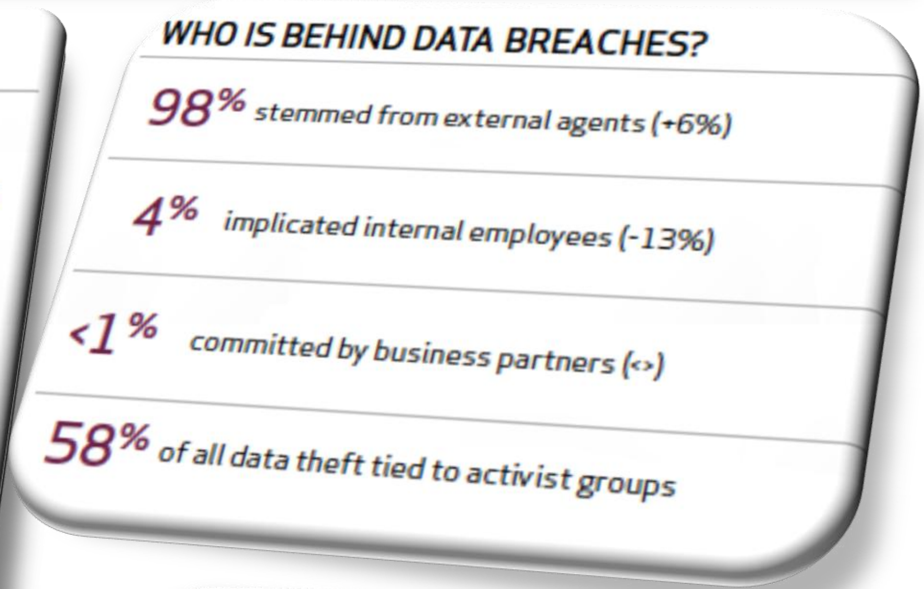
✓ Eliminate unnecessary data; keep tabs on what's left

✓ Ensure essential controls are met; regularly check that they remain so

✓ Monitor and mine event logs

✓ Evaluate your threat landscape to prioritize your treatment strategy

✓ Refer to the conclusion of this report for indicators and mitigators for the most common threats



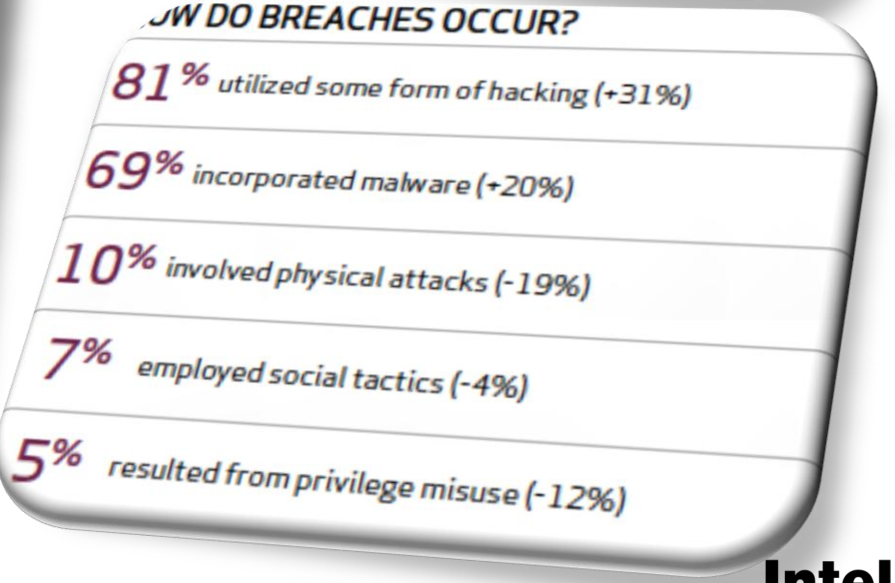
WHO IS BEHIND DATA BREACHES?

98% stemmed from external agents (+6%)

4% implicated internal employees (-13%)

<1% committed by business partners (<>)

58% of all data theft tied to activist groups



..W DO BREACHES OCCUR?

81% utilized some form of hacking (+31%)

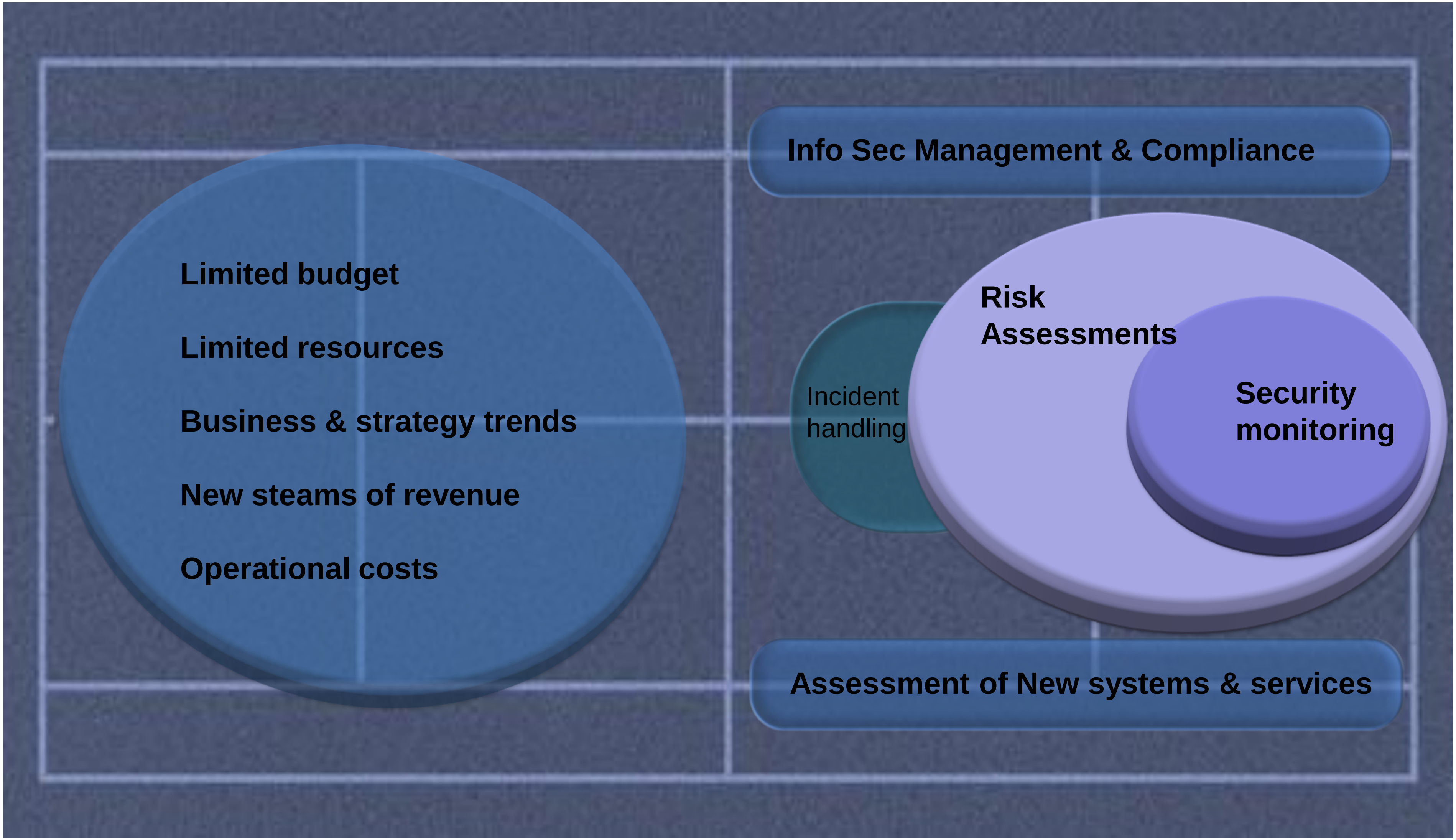
69% incorporated malware (+20%)

10% involved physical attacks (-19%)

7% employed social tactics (-4%)

5% resulted from privilege misuse (-12%)

Setting the playground – info security operation



Limited budget

Limited resources

Business & strategy trends

New steams of revenue

Operational costs

Info Sec Management & Compliance

Incident handling

Risk Assessments

Security monitoring

Assessment of New systems & services

Setting the playground – you’ re not the only one

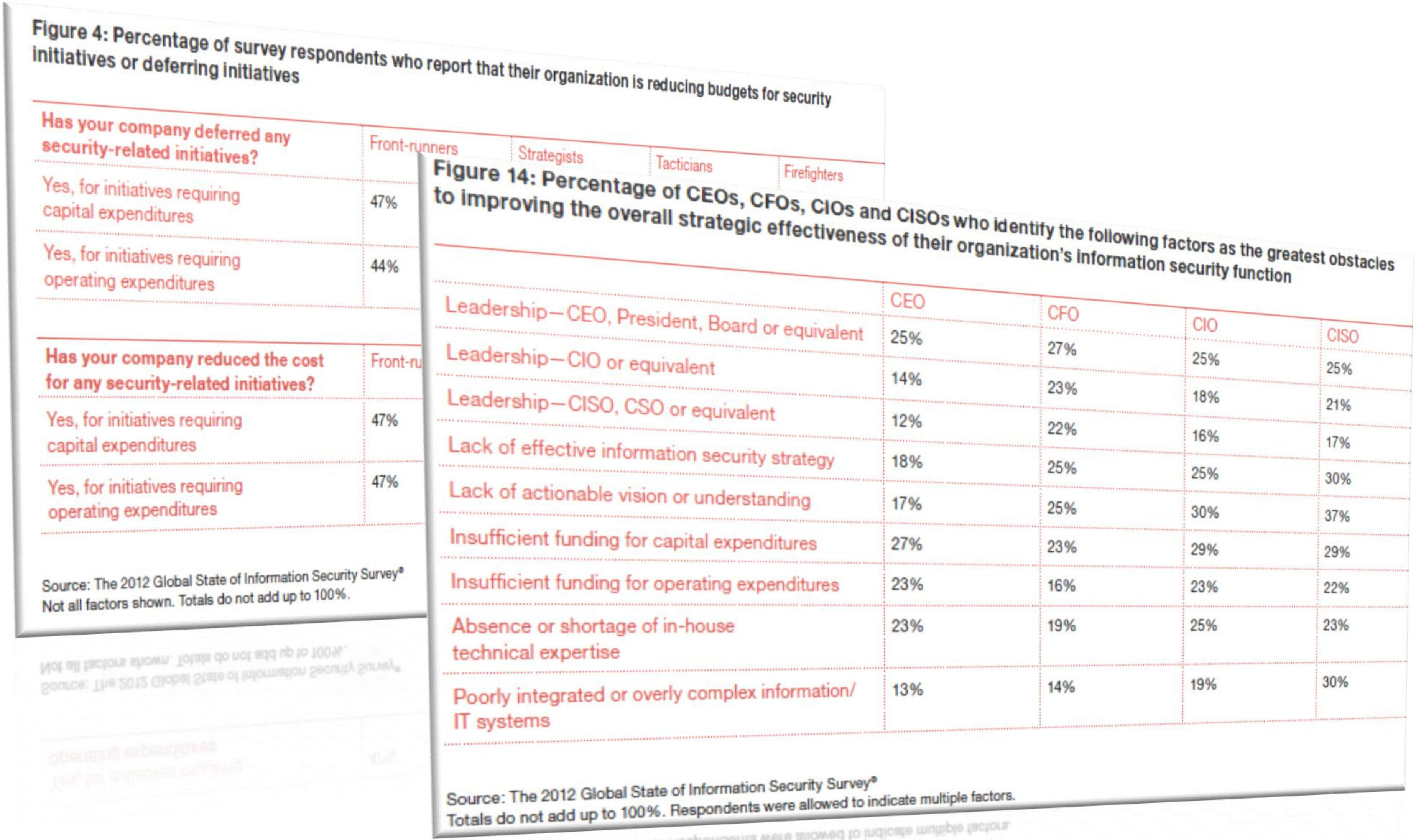


Figure 4: Percentage of survey respondents who report that their organization is reducing budgets for security initiatives or deferring initiatives

Has your company deferred any security-related initiatives?	Front-runners	Strategists	Tacticians	Firefighters
Yes, for initiatives requiring capital expenditures	47%			
Yes, for initiatives requiring operating expenditures	44%			

Has your company reduced the cost for any security-related initiatives?	Front-ru
Yes, for initiatives requiring capital expenditures	47%
Yes, for initiatives requiring operating expenditures	47%

Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

Figure 14: Percentage of CEOs, CFOs, CIOs and CISOs who identify the following factors as the greatest obstacles to improving the overall strategic effectiveness of their organization’s information security function

	CEO	CFO	CIO	CISO
Leadership—CEO, President, Board or equivalent	25%	27%	25%	25%
Leadership—CIO or equivalent	14%	23%	18%	21%
Leadership—CISO, CSO or equivalent	12%	22%	16%	17%
Lack of effective information security strategy	18%	25%	25%	30%
Lack of actionable vision or understanding	17%	25%	30%	37%
Insufficient funding for capital expenditures	27%	23%	29%	29%
Insufficient funding for operating expenditures	23%	16%	23%	22%
Absence or shortage of in-house technical expertise	23%	19%	25%	23%
Poorly integrated or overly complex information/ IT systems	13%	14%	19%	30%

Source: The 2012 Global State of Information Security Survey®
Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

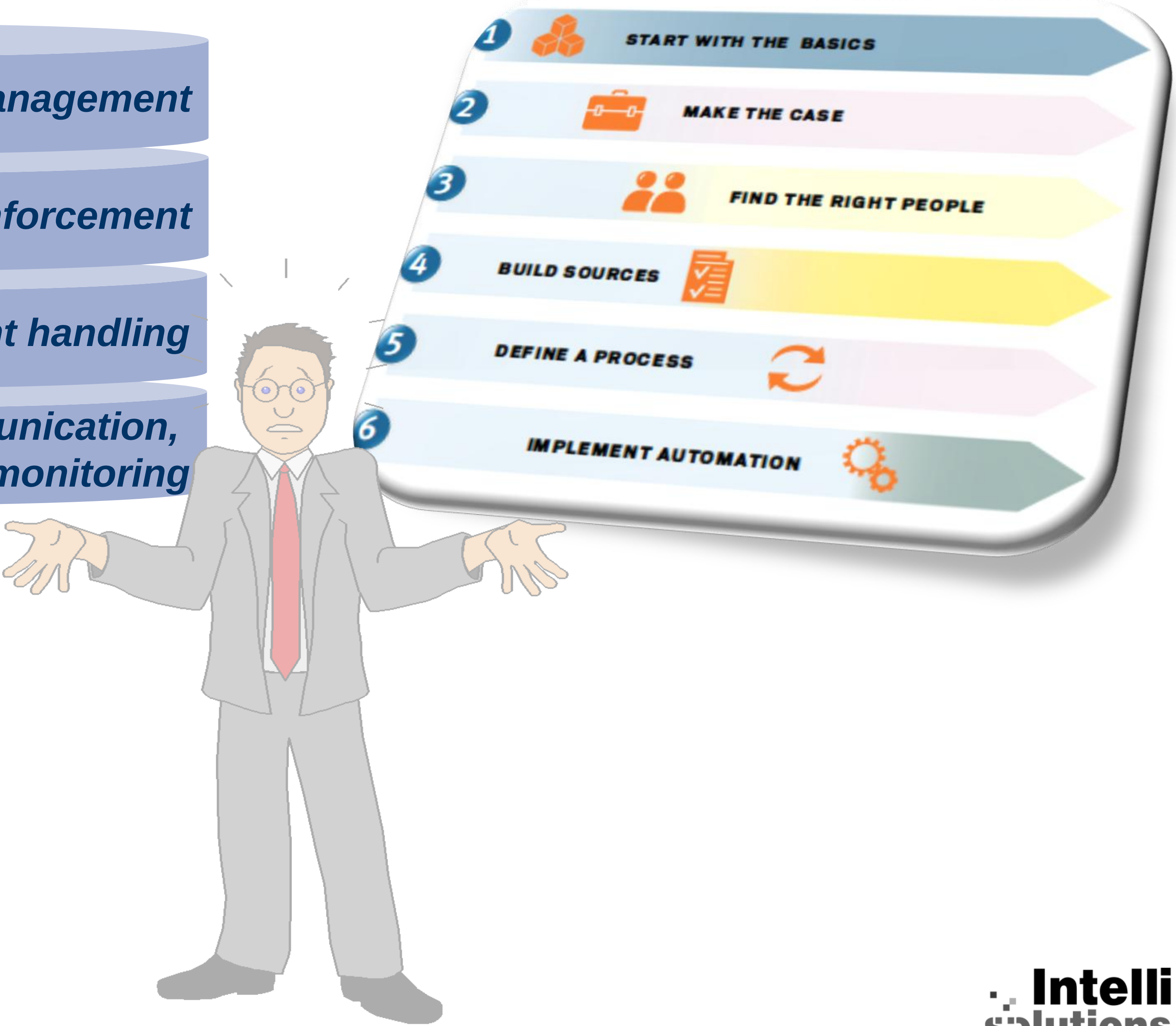
No problem, You can win it …… all

Info Security Risk Management

ISMS adoption & enforcement

Incident handling

Reporting, communication, monitoring

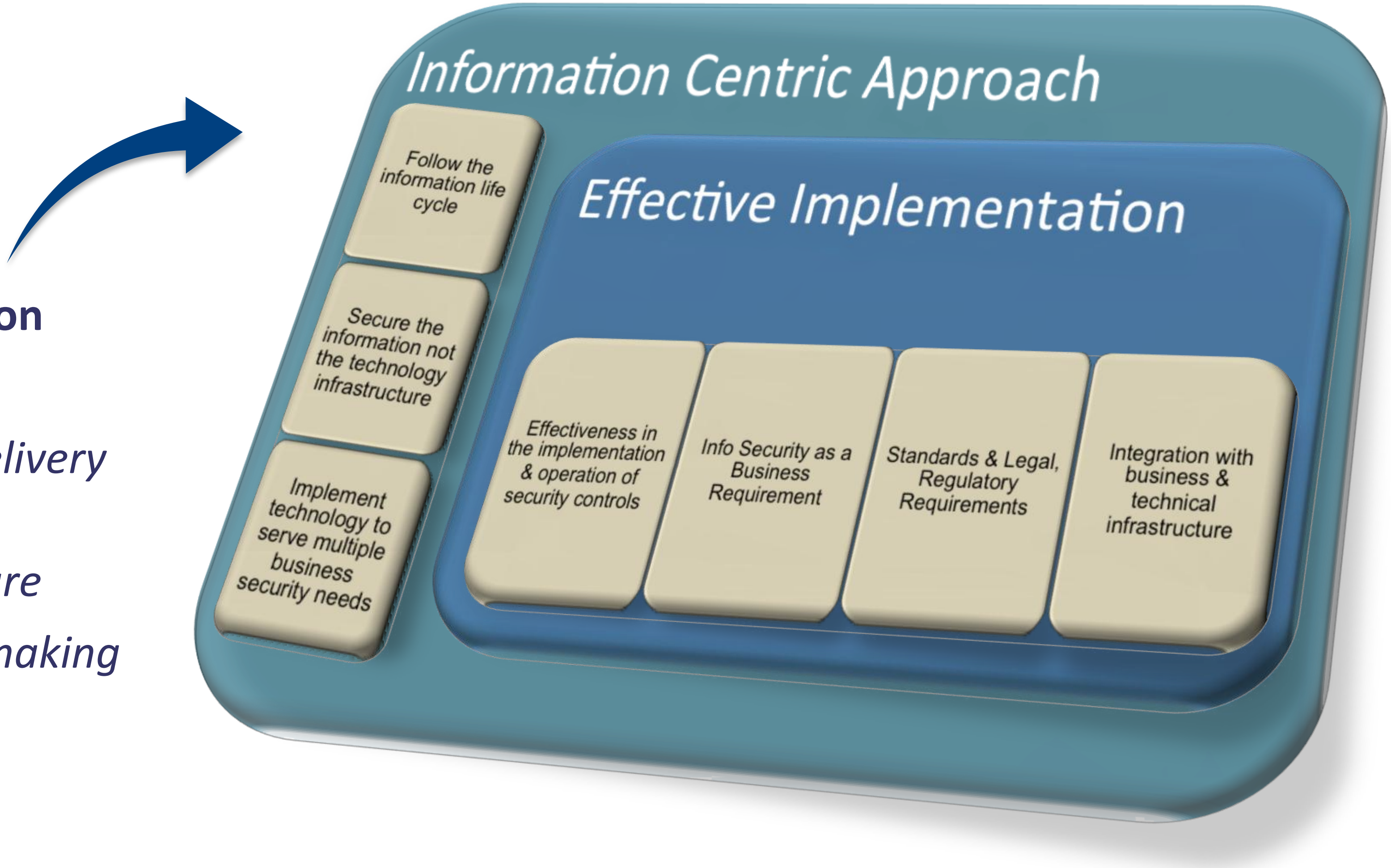


1. START WITH THE BASICS
2. MAKE THE CASE
3. FIND THE RIGHT PEOPLE
4. BUILD SOURCES
5. DEFINE A PROCESS
6. IMPLEMENT AUTOMATION

You can try to win it …… but not all !

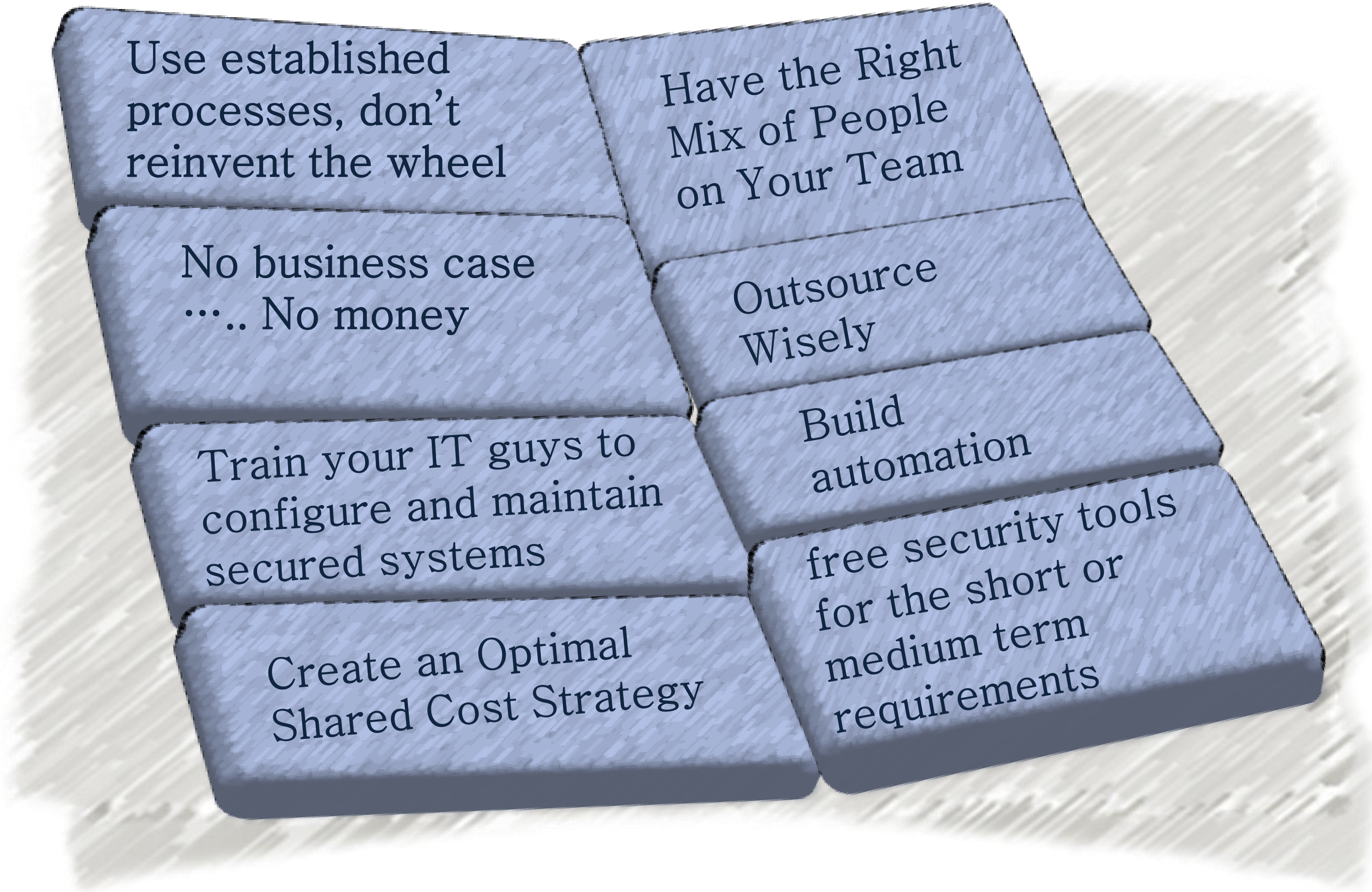
Transformation

- ❑ *Cultural*
- ❑ *Service Delivery*
- ❑ *Solutions Architecture*
- ❑ *Decision making*



Information Centric Approach
Follow the information life cycle
Secure the information not the technology infrastructure
Implement technology to serve multiple business security needs
Effective Implementation
Effectiveness in the implementation & operation of security controls
Info Security as a Business Requirement
Standards & Legal, Regulatory Requirements
Integration with business & technical infrastructure

You can try to win it …… but not all !



Use established processes, don’t reinvent the wheel

Have the Right Mix of People on Your Team

No business case ….. No money

Outsource Wisely

Train your IT guys to configure and maintain secured systems

Build automation

Create an Optimal Shared Cost Strategy

free security tools for the short or medium term requirements

You can try to win it …… but not all !

Logging out:

- Communication is the key
- Prove added value of info security
- A good business case is required to get approval especially at this time when money is hard to earn (minimize operational costs, compliance, assist in building new streams of revenue)
- Not everything is important
- Management of compliance process & required activities

Thank You

Q&A

PASSION – EXPERIENCE – INNOVATION - INTEGRITY – PROFESSIONALISM - COMMITMENT

Intelli
solutions
TRUSTED IT ADVISOR