Business Satisfaction and Alignment

REPORT

PREPARED FOR:

Joe Computerguy
Computer Business Inc.

2014-03-21

IT SECURITY
DIAGNOSTIC PROGRAM
POWERED BY INFO-TECH RESEARCH GROUP

INFO~TECH
RESEARCH GROUP

Business Satisfaction with IT Security

Computer Business Inc.

Business Responses Only

# of Employees	37
# of Responses	37
Response Rate	100.0%

powered by INFO-TECH RESEARCH GROUP

Business satisfaction is defined as confidence in important security areas and minimal friction for business processes.

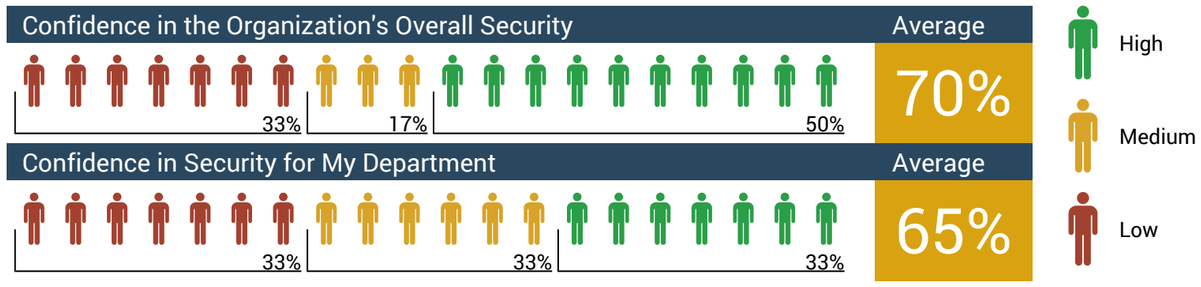
Security Importance and Confidence

Identify the business perspective on security importance and confidence at the department and organizational level. Low importance scores for "My Department" might reflect under-valuing their own day-to-day security practices. Similarly, low confidence scores might reveal hidden vulnerabilities (e.g., staff sharing passwords).

Importance and Confidence for Overall Security

Overall, how important is IT security to your organization/department?

Overall, how confident are you in the existing IT security practices for your organization/department?

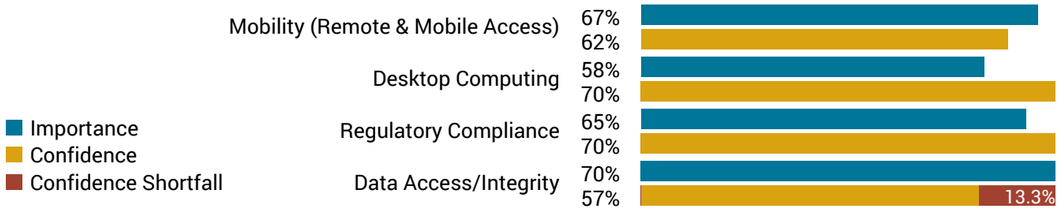


Importance vs. Confidence Detailed Breakdown

Target improvement efforts on areas with high Confidence Shortfalls (i.e., confidence lower than importance).

How important are IT security practices in these areas?

How confident are you in the existing IT security practices in these areas?



Security Friction

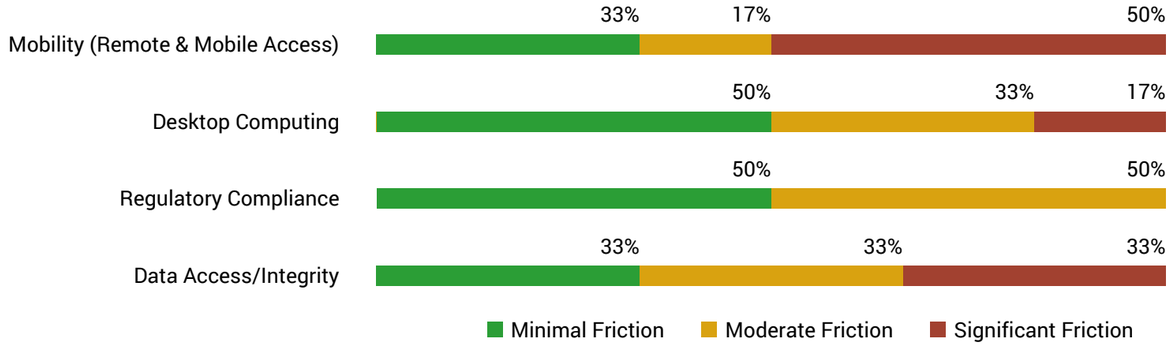
Address high friction areas with the business and modify security practices as necessary.

Security Friction Overall

Overall, how much friction do IT security practices create for business processes?

Security Friction Detailed Breakdown

How much do the IT security practices in these areas create friction for business processes?



Responsibility for Security Governance

Shared IT-business responsibility for security governance (e.g., risk analysis) leads to better alignment and greater understanding of risk tolerance, security priorities, and acceptable security practices.

Who should have responsibility for these IT security governance areas?

IT Satisfaction with IT Security

Computer Business Inc.

IT Responses Only

# of Employees	18
# of Responses	18
Response Rate	100.0%

powered by INFO-TECH RESEARCH GROUP

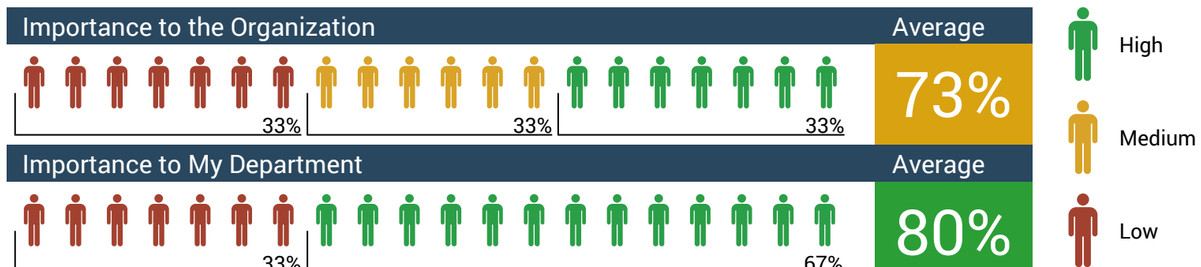
Business satisfaction is defined as confidence in important security areas and minimal friction for business processes.

Security Importance and Confidence

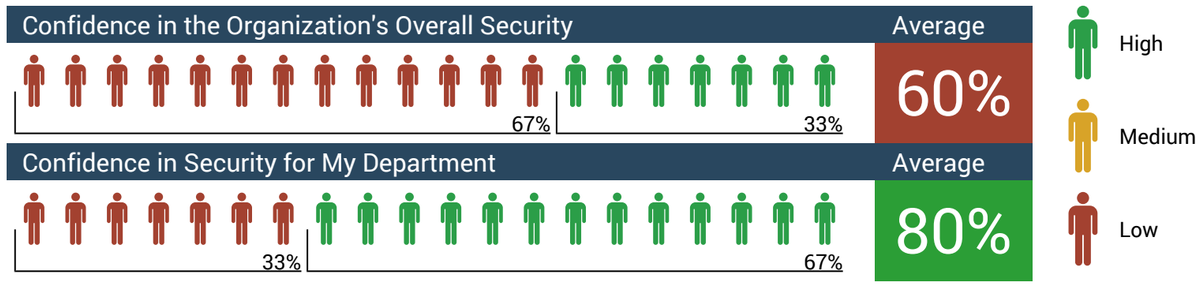
Identify the business perspective on security importance and confidence at the department and organizational level. Low importance scores for "My Department" might reflect under-valuing their own day-to-day security practices. Similarly, low confidence scores might reveal hidden vulnerabilities (e.g., staff sharing passwords).

Importance and Confidence for Overall Security

Overall, how important is IT security to your organization/department?



Overall, how confident are you in the existing IT security practices for your organization/department?

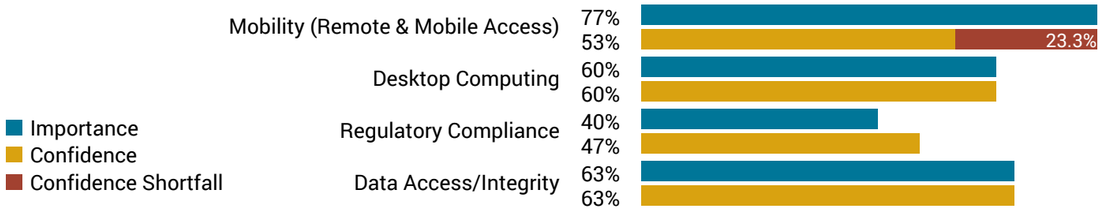


Importance vs. Confidence Detailed Breakdown

Target improvement efforts on areas with high Confidence Shortfalls (i.e., confidence lower than importance).

How important are IT security practices in these areas?

How confident are you in the existing IT security practices in these areas?



Security Friction

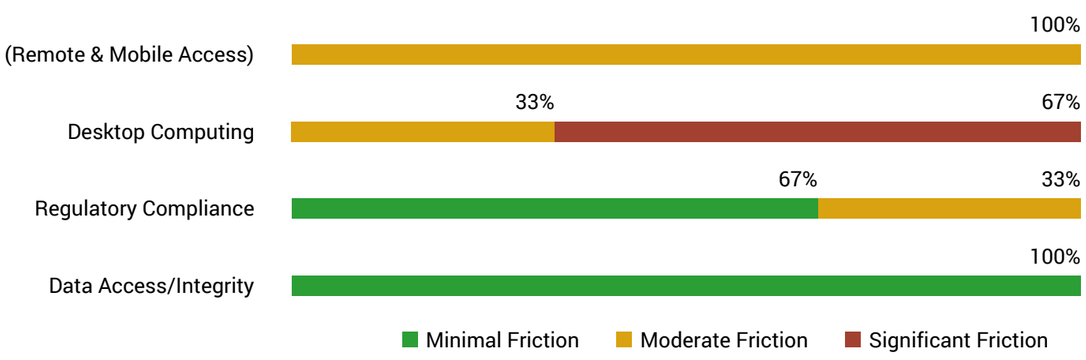
Address high friction areas with the business and modify security practices as necessary.

Security Friction Overall

Overall, how much friction do IT security practices create for business processes?

Security Friction Detailed Breakdown

How much do the IT security practices in these areas create friction for business processes?



Responsibility for Security Governance

Shared IT-business responsibility for security governance (e.g., risk analysis) leads to better alignment and greater understanding of risk tolerance, security priorities, and acceptable security practices.

Who should have responsibility for these IT security governance areas?

IT-Business Alignment

Computer Business Inc.

IT & Business Responses

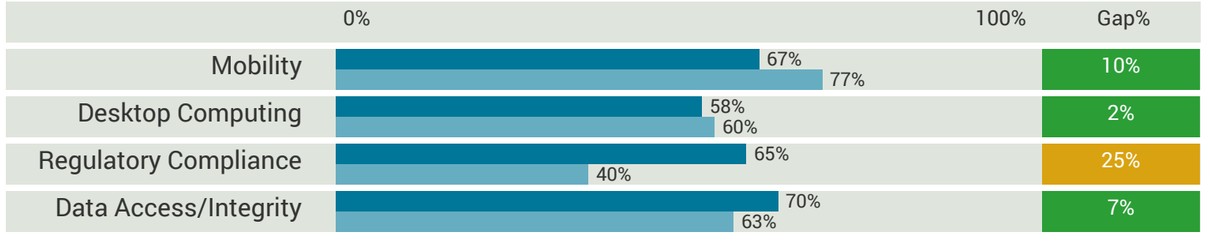
# of Employees	55
# of Responses	55
Response Rate	100.0%

powered by INFO~TECH RESEARCH GROUP

Identify gaps between IT and the business, and use that to drive alignment exercises.

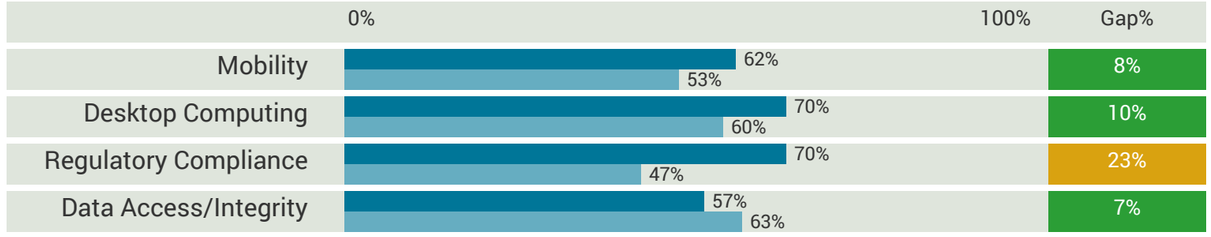
Security Importance

How important are IT security practices in these areas? Business's Response | IT's Response



Security Confidence

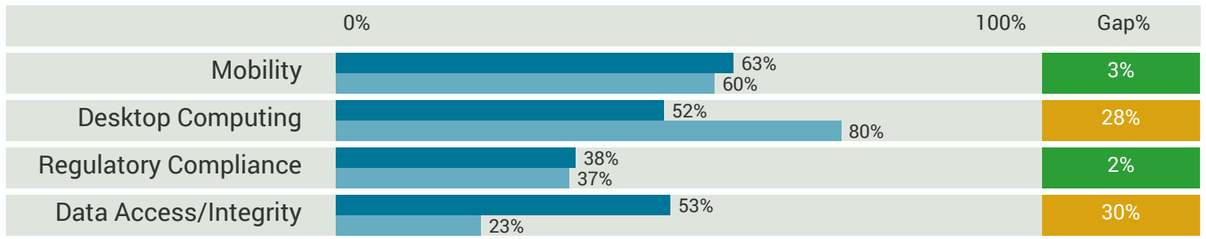
How confident are you in the existing IT security practices in these areas? Business's Response | IT's Response



GAP LEGEND | 0-15% Well-Aligned | 16-30% Review and Consider Alignment Exercise | 31+ % Conduct Alignment Exercise

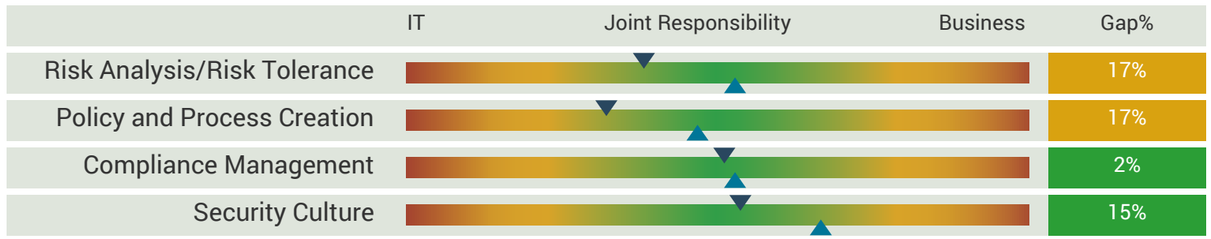
Security Friction

How much do the IT security practices in these areas create friction for business processes? Business's Response | IT's Response



Responsibility for Security Governance

Who should have responsibility for these IT security governance areas? ▲ IT ▼ Business



Follow These Steps to Close Gaps and Improve Satisfaction

1. **Meet with business users to explore scores that are misaligned** – e.g., are confidence gaps due to perception only or are concerns founded in sub-optimal security practices?

2. For importance and confidence gaps, **identify the root cause and review related practices.** For example, if mobility confidence is low, is the underlying concern protecting data on mobile devices or preventing malware attacks? Similarly, if mobility security has a high importance score due to data concerns, then also review overall data access/integrity security concerns.

3. For security satisfaction low scores and gaps, **identify the specific practices that are deemed too restrictive or cumbersome, and the underlying causes of dissatisfaction.** For example, if remote access friction is actually due to usability issues with the VPN client and not security policies, then the issue may be solved by exploring alternative VPN client solutions. In other cases, it may be necessary to re-align end-user perspectives on security requirements.

4. For governance responsibility gaps, **determine the potential points of friction (e.g., time commitment) to move towards joint responsibility** so you can have an informed discussion of what is appropriate. For example, joint responsibility does not mean identical time commitments. In risk analysis, for example, it's still IT's responsibility to identify and present risks and mitigation options; the business role is to provide feedback on risk tolerance.

5. **Leverage Info-Tech's Security Effectiveness reports** for a deeper review of security practices.

Satisfaction by Department

Computer Business Inc.

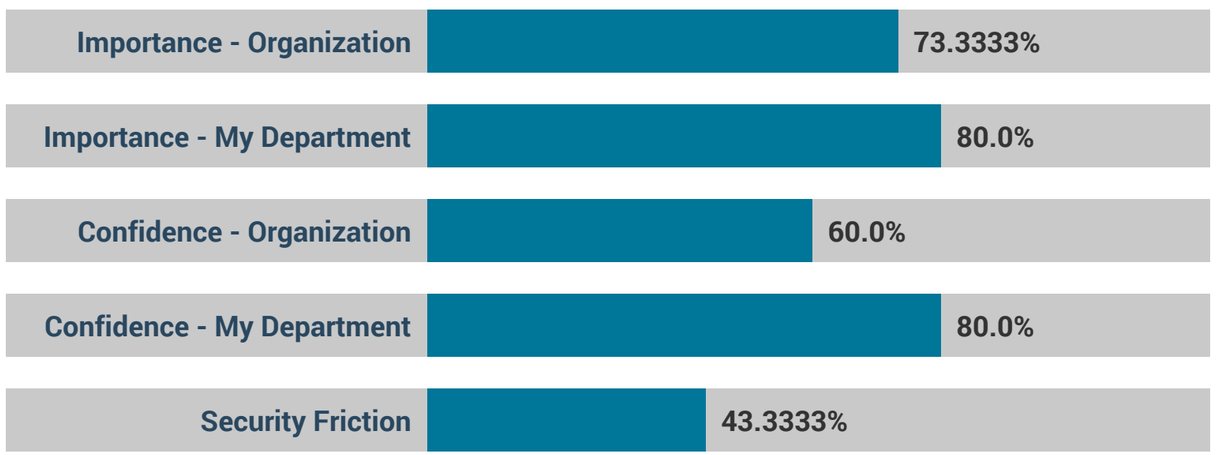
IT & Business Responses

# of Employees	55
# of Responses	55
Response Rate	100.0%

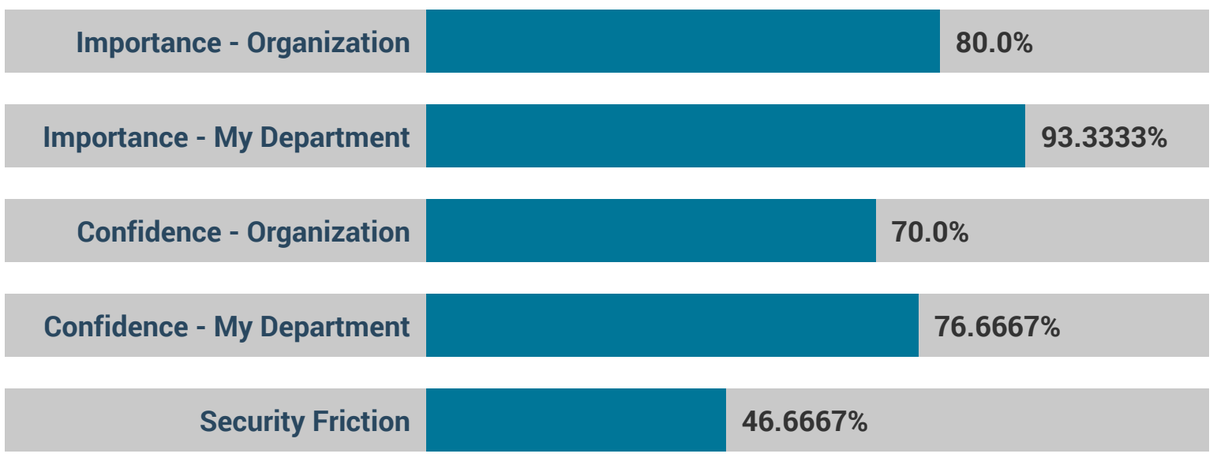
powered by INFO~TECH RESEARCH GROUP

The overall Importance, Confidence, and Friction scores by department are provided below. For a detailed breakdown, see the Department View pages.

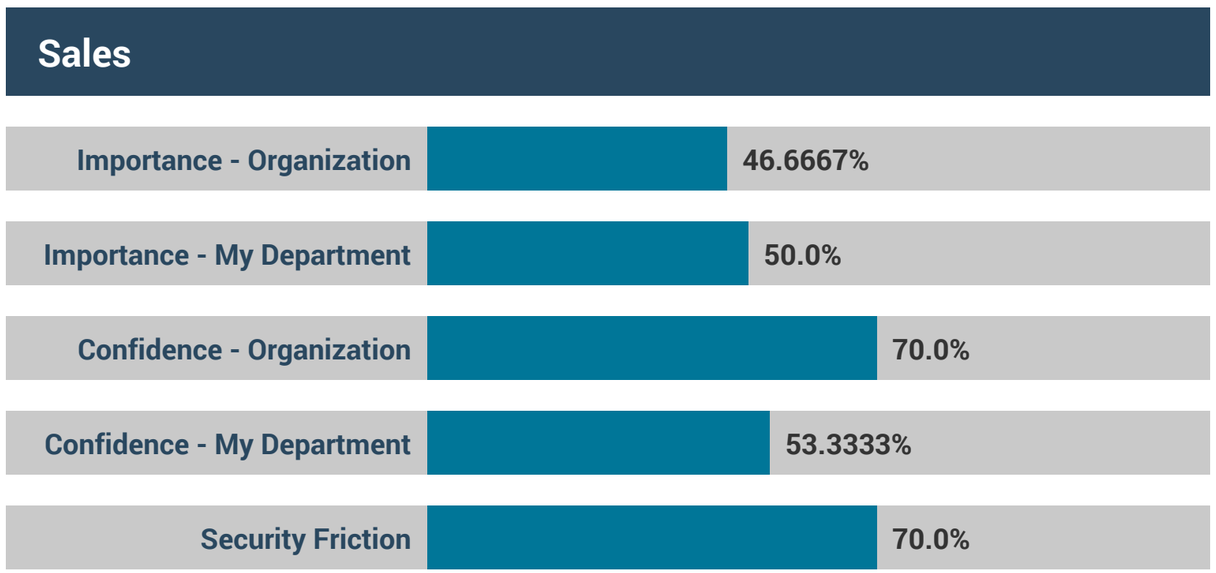
IT



Finance



Sales



Department View:
Finance Satisfaction with IT Security

Computer Business Inc.

# of Employees	3
# of Responses	3
Response Rate	100.0%

powered by INFO~TECH RESEARCH GROUP

Business satisfaction is defined as confidence in important security areas and minimal friction for business processes.

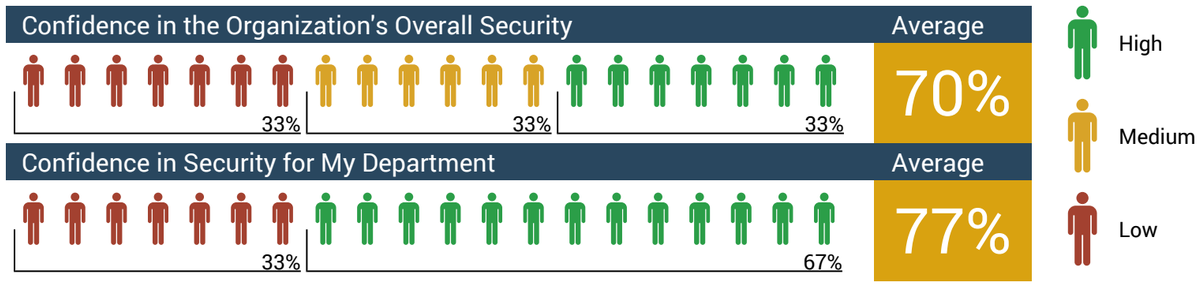
Security Importance and Confidence

Identify the business perspective on security importance and confidence at the department and organizational level. Low importance scores for "My Department" might reflect under-valuing their own day-to-day security practices. Similarly, low confidence scores might reveal hidden vulnerabilities (e.g., staff sharing passwords).

Importance and Confidence for Overall Security

Overall, how important is IT security to your organization/department?

Overall, how confident are you in the existing IT security practices for your organization/department?

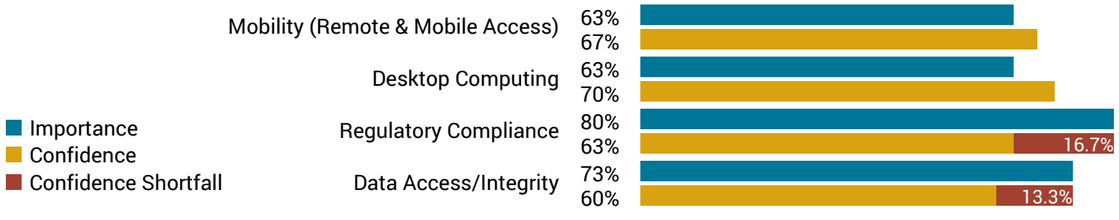


Importance vs. Confidence Detailed Breakdown

Target improvement efforts on areas with high Confidence Shortfalls (i.e., confidence lower than importance).

How important are IT security practices in these areas?

How confident are you in the existing IT security practices in these areas?



Security Friction

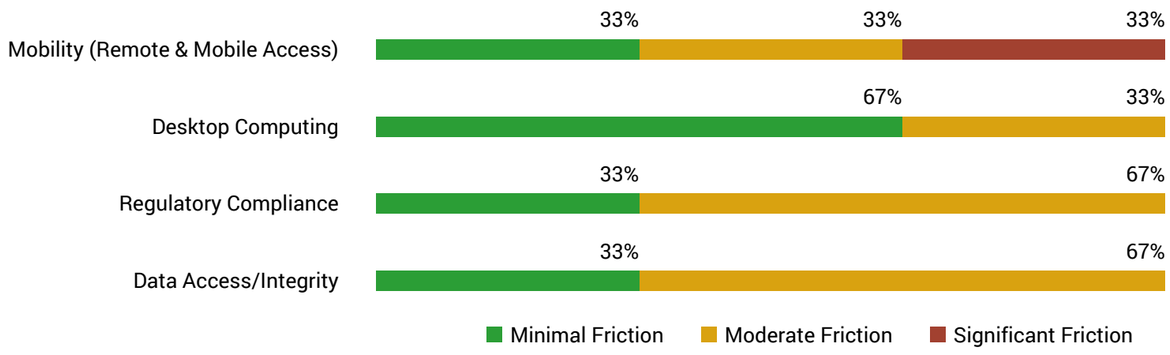
Address high friction areas with the business and modify security practices as necessary.

Security Friction Overall

Overall, how much friction do IT security practices create for business processes?

Security Friction Detailed Breakdown

How much do the IT security practices in these areas create friction for business processes?



Responsibility for Security Governance

Shared IT-business responsibility for security governance (e.g., risk analysis) leads to better alignment and greater understanding of risk tolerance, security priorities, and acceptable security practices.

Who should have responsibility for these IT security governance areas?

Department View:
Sales Satisfaction with IT Security

Computer Business Inc.

# of Employees	34
# of Responses	34
Response Rate	100.0%

powered by INFO~TECH RESEARCH GROUP

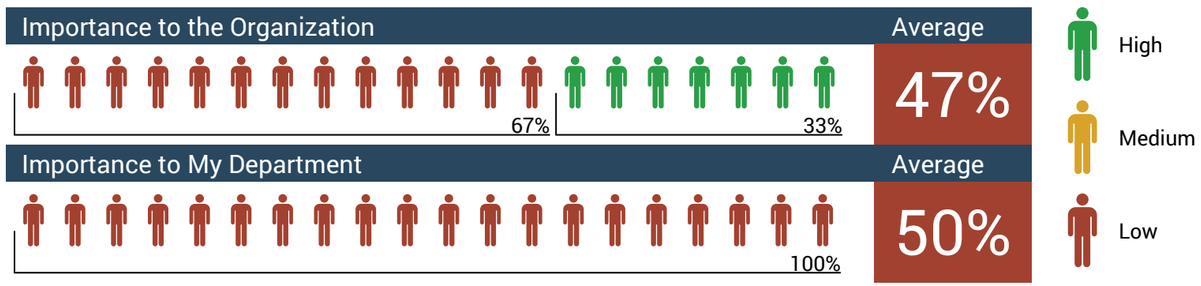
Business satisfaction is defined as confidence in important security areas and minimal friction for business processes.

Security Importance and Confidence

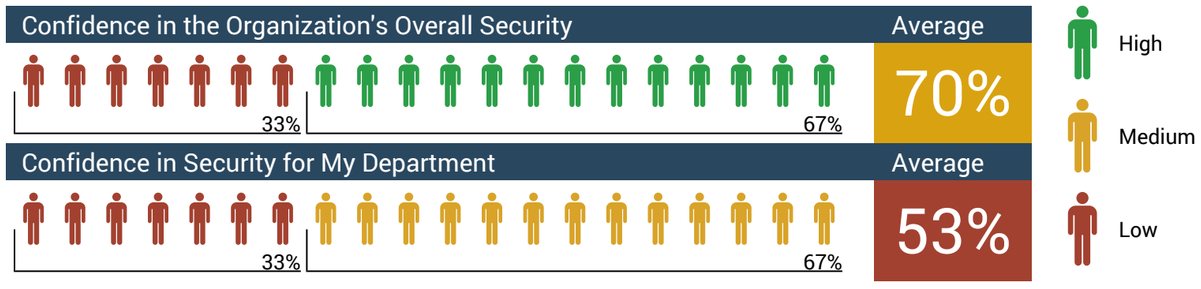
Identify the business perspective on security importance and confidence at the department and organizational level. Low importance scores for "My Department" might reflect under-valuing their own day-to-day security practices. Similarly, low confidence scores might reveal hidden vulnerabilities (e.g., staff sharing passwords).

Importance and Confidence for Overall Security

Overall, how important is IT security to your organization/department?



Overall, how confident are you in the existing IT security practices for your organization/department?

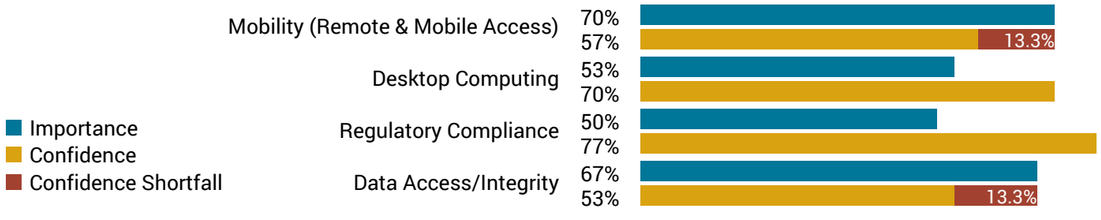


Importance vs. Confidence Detailed Breakdown

Target improvement efforts on areas with high Confidence Shortfalls (i.e., confidence lower than importance).

How important are IT security practices in these areas?

How confident are you in the existing IT security practices in these areas?



Security Friction

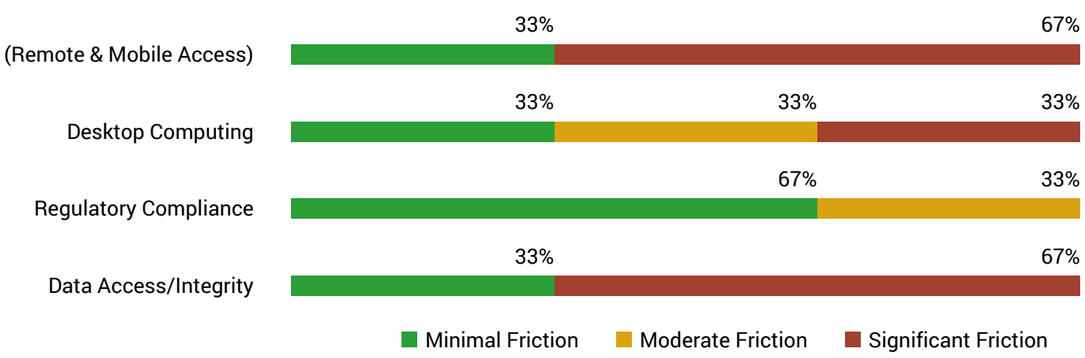
Address high friction areas with the business and modify security practices as necessary.

Security Friction Overall

Overall, how much friction do IT security practices create for business processes?

Security Friction Detailed Breakdown

How much do the IT security practices in these areas create friction for business processes?



Responsibility for Security Governance

Shared IT-business responsibility for security governance (e.g., risk analysis) leads to better alignment and greater understanding of risk tolerance, security priorities, and acceptable security practices.

Who should have responsibility for these IT security governance areas?

What is the biggest pain point in terms of IT security interfering with your work? What would you like to see done differently?

FINANCE

Luke Stewart - Comment text

Danny Black - Comment text

Debbie Slater - Comment text

SALES

Susan Jones - Comment text

Sandy Richardson - Comment text

John Robert - Comment text

IT

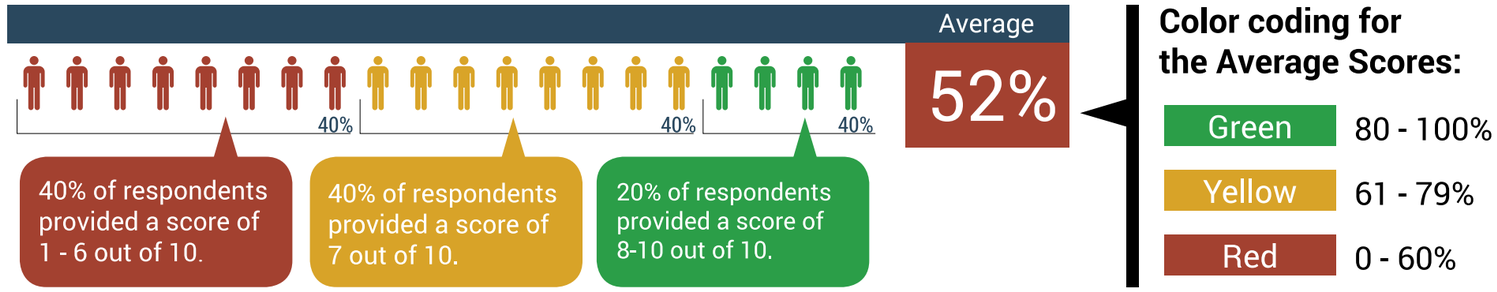
Bob Smith - Comment text

Mike Brown - Comment text

Bonnie Cook - Comment text

Importance and Confidence

This chart type is used to present a breakdown of responses as well as an overall average score.



Security Friction

For security friction, a high score indicates high friction, which is a negative result. Therefore a high score is color-coded as red (not green).

Responsibility for Security Governance

Security governance is improved when there is joint responsibility between IT and the business. Therefore, a middle score is a positive result and is color-coded as green.