INTERNATIONAL TRENDS IN CYBERSECURITY

Overview

April 2016

EXECUTIVE SUMMARY

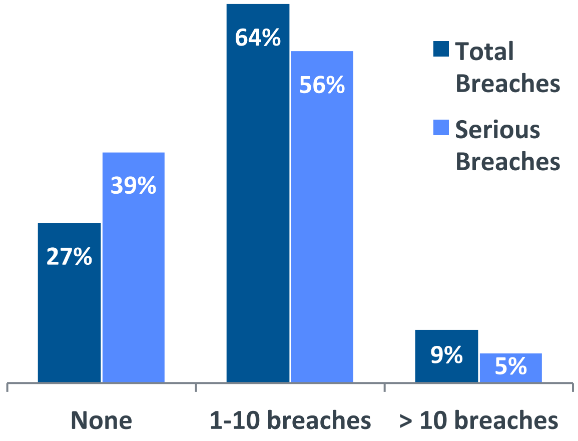
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In most of the countries surveyed, one of the greatest factors has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms, as well as internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/incident* in the past 12 months (73%).

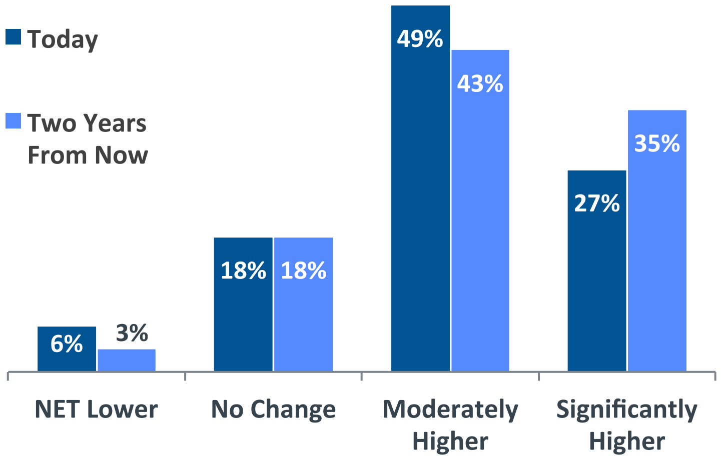
OCCURRENCE OF SECURITY BREACHES

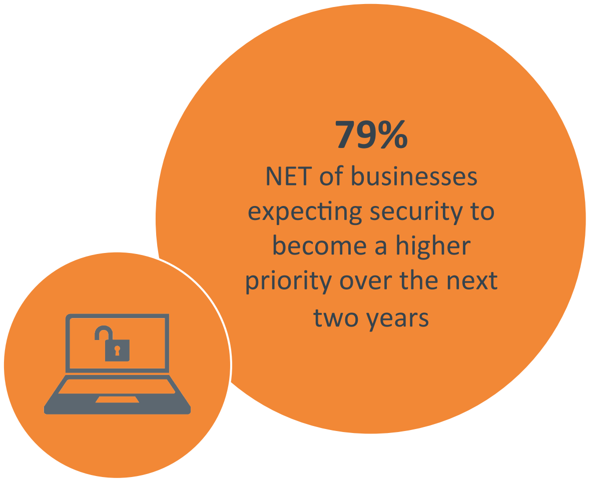
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY





79%
NET of businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

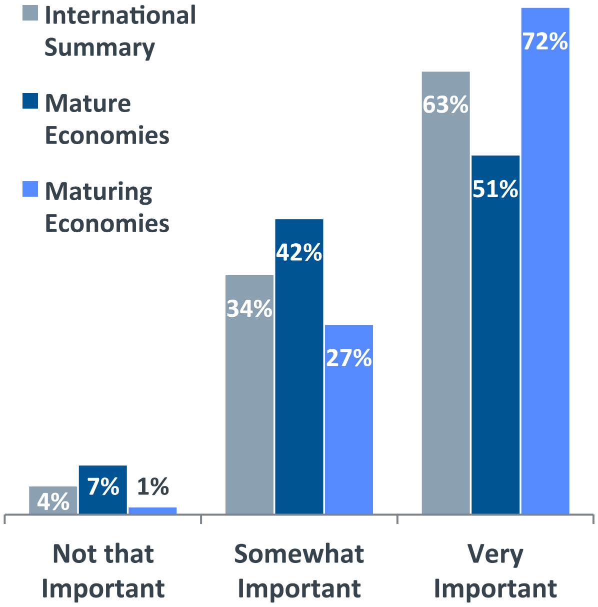
1. Change in IT operations (e.g. cloud, mobility)
2. Reports of security breaches at other firms
3. Internal security breach or incident
4. Change in business operations or client base
5. Knowledge gained from training/certification

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

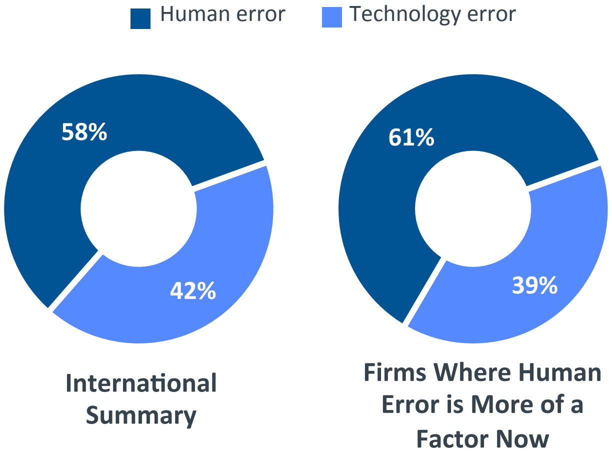
While nearly three-quarters of organizations report experiencing at least one security incident, about 6 in 10 had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies now vs. two years ago, especially for those in Maturing Economies (64% net overall significantly more + moderately more).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (96% net very important + somewhat important). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Overall, 8 in 10 managers indicate that IT security certifications are very valuable (38%) or valuable (42%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

1. General carelessness
2. Failure to get up to speed on new threats
3. Lack of expertise with websites and applications
4. End user failure to follow policies and procedures
5. Lack of expertise with networks, servers and other infrastructure
6. IT staff failure to follow policies and procedures

76%

% of firms reporting a mobile related security incident. Top issues: lost device, mobile malware, and mobile phishing attacks.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Australia

April 2016

EXECUTIVE SUMMARY

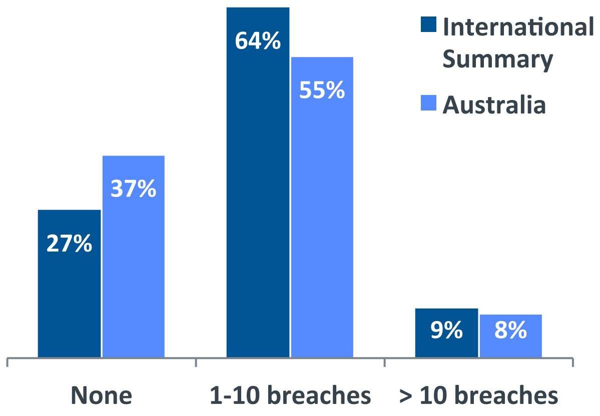
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly three-quarters of businesses in Australia expect IT security to grow in importance (72% net higher).

Due to the evolving nature of IT, the great majority of organisations have had to respond by changing the way their company approaches security. In Australia, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms as well as internal incidents. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

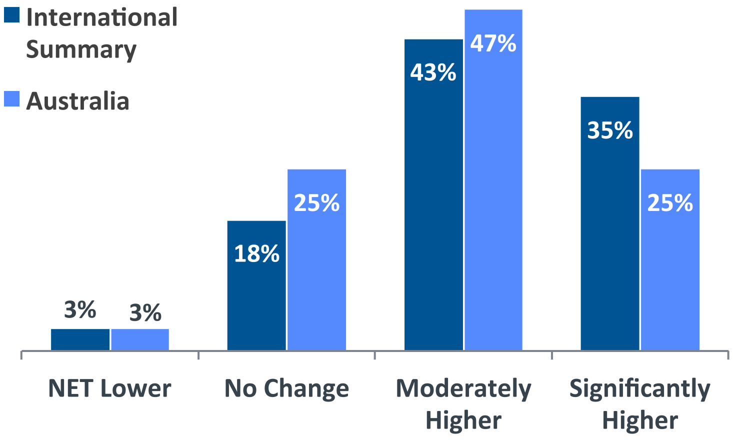
Over the past 12 months

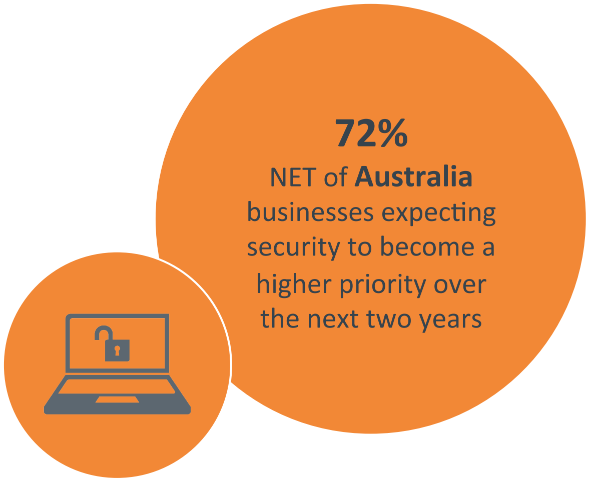


*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today





72%
NET of **Australia** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Australia businesses

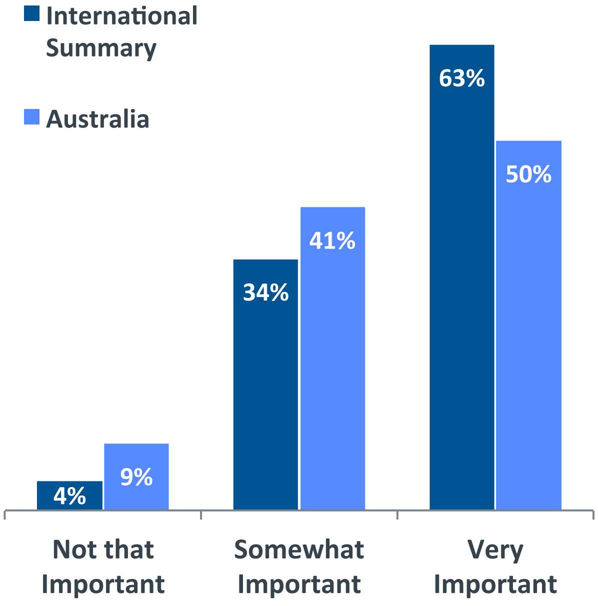
1. Change in IT operations (e.g. cloud, mobility)
2. Reports of security breaches at other firms
3. Internal security breach or incident
4. Knowledge gained from training/certification
5. Change in business operations or client base

Note: see the last page for which countries are categorised in Maturing Economies vs. Mature Economies.

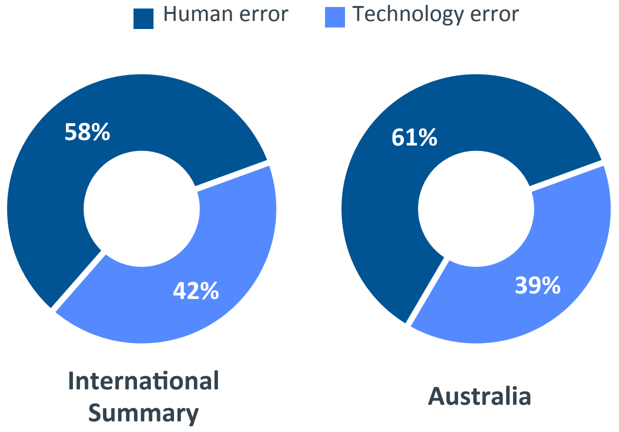
While 6 in 10 Australian organisations experienced at least one security incident, slightly more than a half had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Australia, it is more of a factor now vs. two years ago for more than half (56% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 89% in Australia). And most managers believe it is important to test after IT security training to confirm knowledge gains (91% net very important + somewhat important in Australia). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Seven in ten Australian managers indicate that IT security certifications are very valuable (24%) or valuable (47%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Australia businesses

1. Failure to get up to speed on new threats
2. End user failure to follow policies and procedures
3. General carelessness
4. Intentional disabling of security
5. Lack of expertise with websites and applications
6. IT staff failure to follow policies and procedures

71%
% of **Australia** businesses reporting a mobile related security incident. Top issues: lost device, data policy violation, and staff disabling security features

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Brazil

April 2016

EXECUTIVE SUMMARY

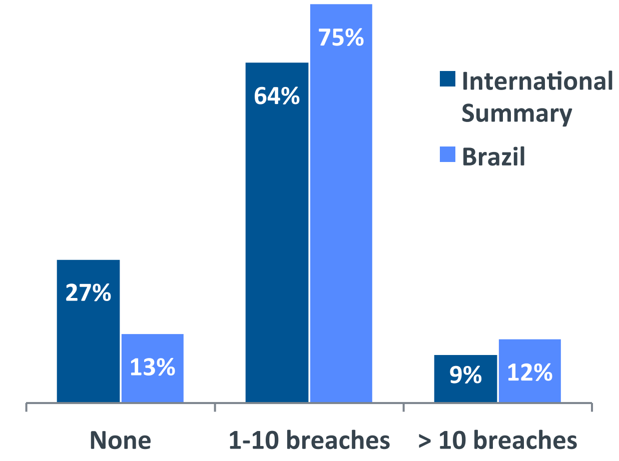
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nine in ten businesses in Brazil expect IT security to grow in importance (90% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Brazil, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

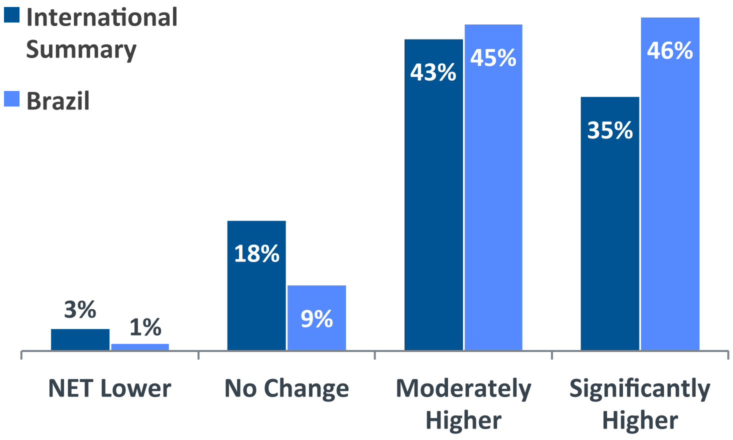
Over the past 12 months

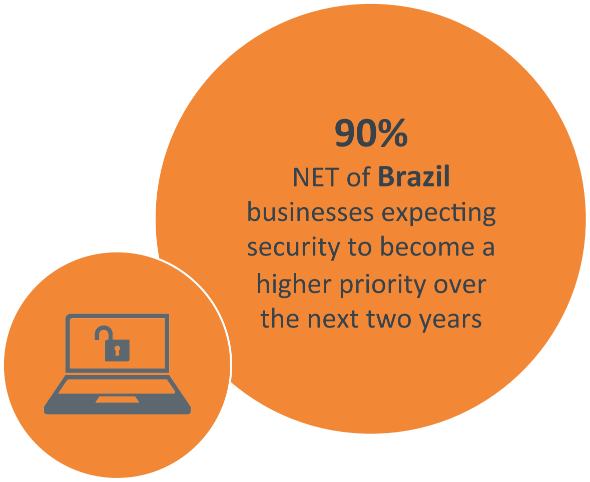


*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today





90%

NET of **Brazil** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Brazil businesses

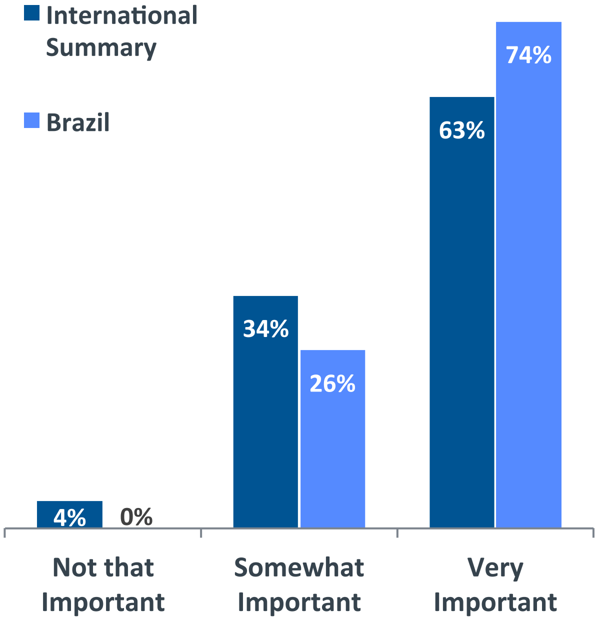
1. Change in IT operations (e.g. cloud, mobility)
2. Change in business operations or client base
3. Knowledge gained from training/certification
4. Focus on a new industry vertical
5. Reports of security breaches at other firms

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

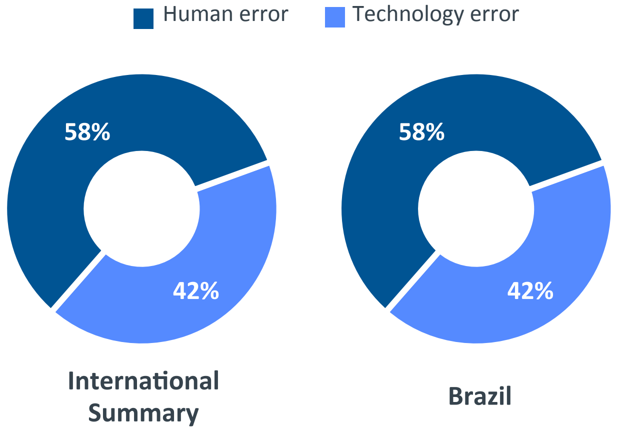
While nearly 9 in 10 Brazil organizations experienced at least one security incident, slightly over three-quarters had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Brazil, it is more of a factor now vs. two years ago for nearly three-quarters of businesses (72% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 94% in Brazil). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (100% net very important + somewhat important in Brazil). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Most Brazil managers indicate that IT security certifications are very valuable (71%) or valuable (22%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Brazil businesses

1. General carelessness
2. IT staff failure to follow policies and procedures
3. Failure to get up to speed on new threats
4. End user failure to follow policies and procedures
5. Lack of expertise with networks, servers and other infrastructure
6. Lack of expertise with websites and applications

81%

% of **Brazil** businesses reporting a mobile related security incident. Top issues: lost device, mobile malware, and mobile phishing attacks.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Canada

April 2016

EXECUTIVE SUMMARY

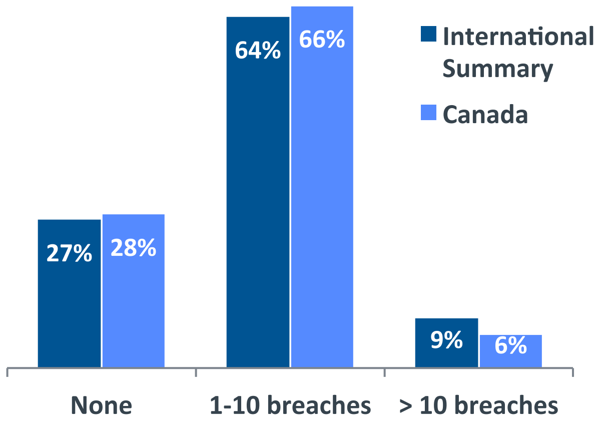
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly two-thirds of businesses in Canada expect IT security to grow in importance (67% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Canada, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms as well as internal incidents. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

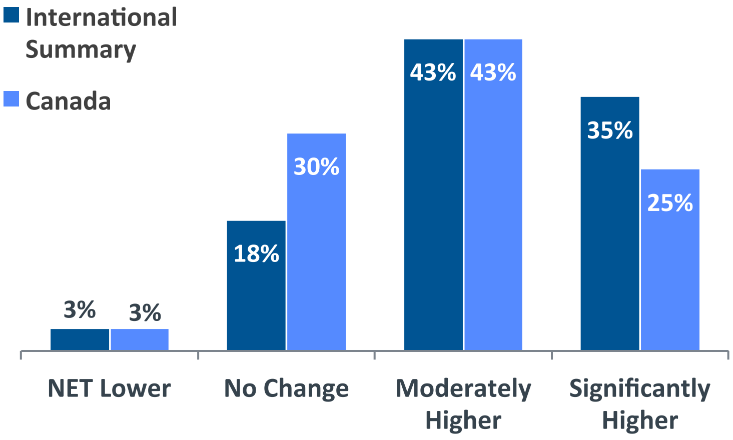
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



67%
NET of **Canada** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Canada businesses

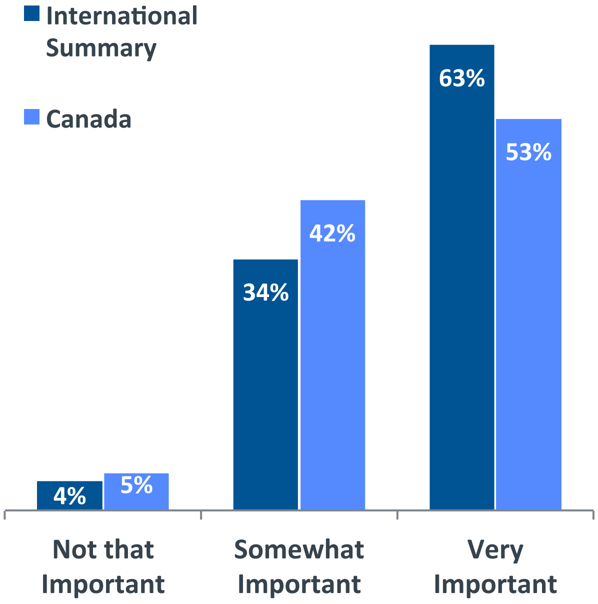
1. Change in IT operations (e.g. cloud, mobility)
2. Reports of security breaches at other firms
3. Change in business operations or client base
4. Internal security breach or incident
5. Knowledge gained from training/certification

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

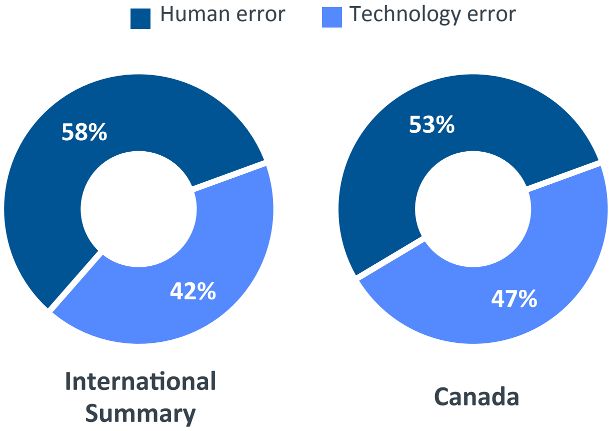
While 7 in 10 Canada organizations experienced at least one security incident, slightly over half had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Canada, it is more of a factor now vs. two years ago for half (50% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 93% in Canada). And most managers believe it is important to test after IT security training to confirm knowledge gains (95% net very important + somewhat important in Canada). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). More than three-quarters of Canada managers indicate that IT security certifications are very valuable (31%) or valuable (47%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Canada businesses

1. General carelessness
2. End user failure to follow policies and procedures
3. Lack of expertise with networks, servers and other infrastructure
4. Lack of expertise with websites and applications
5. IT staff failure to follow policies and procedures
6. Failure to get up to speed on new threats

72%
% of **Canada** firms reporting a mobile related security incident. Top issues: lost device, mobile phishing attacks, and data policy violation.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Germany

April 2016

EXECUTIVE SUMMARY

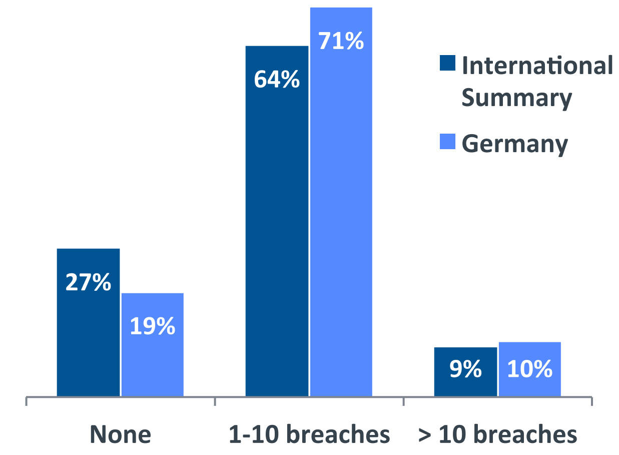
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly three-quarters of businesses in Germany expect IT security to grow in importance (73% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Germany, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms as well as internal incidents. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

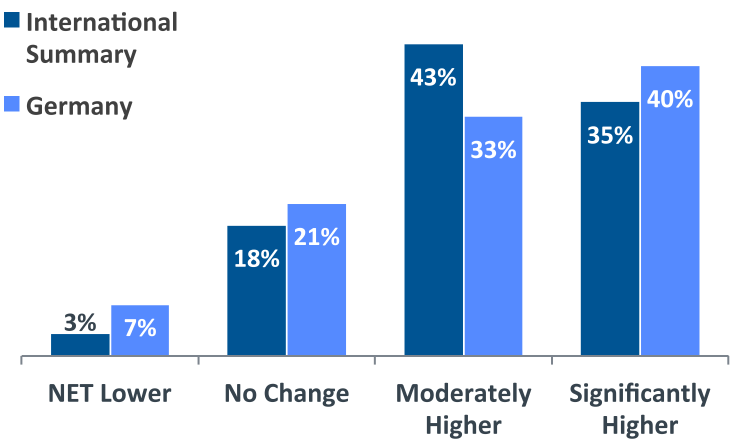
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



73%
NET of **Germany** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Germany businesses

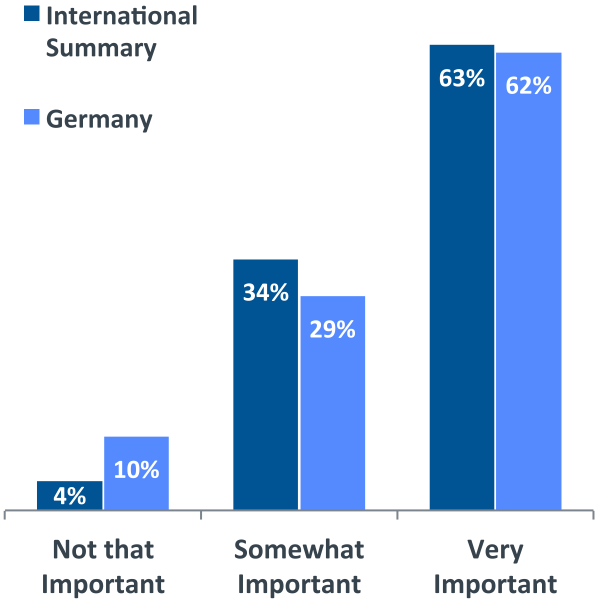
1. Change in IT operations (e.g. cloud, mobility)
2. Knowledge gained from training/certification
3. Reports of security breaches at other firms
4. Internal security breach or incident
5. Change in management

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

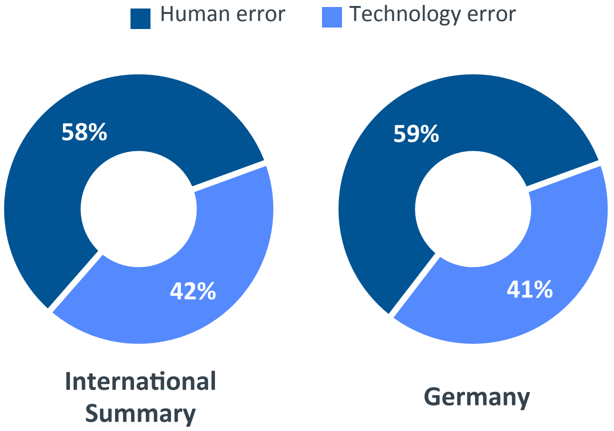
While 8 in 10 organizations in Germany experienced at least one security incident, nearly two-thirds had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Germany, it is more of a factor now vs. two years ago for more than half (63% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 90% in Germany). And most managers believe it is important to test after IT security training to confirm knowledge gains (91% net very important + somewhat important in Germany). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Two-thirds of managers in Germany indicate that IT security certifications are very valuable (23%) or valuable (44%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Germany businesses

1. General carelessness
2. Failure to get up to speed on new threats
3. IT staff failure to follow policies and procedures
4. End user failure to follow policies and procedures
5. Lack of expertise with networks, servers and other infrastructure
6. Inadequate resources/lack of time to manage threats

76%
% of **Germany** businesses reporting a mobile related security incident. Top issues: lost device, mobile malware, and data policy violation.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for India

April 2016

EXECUTIVE SUMMARY

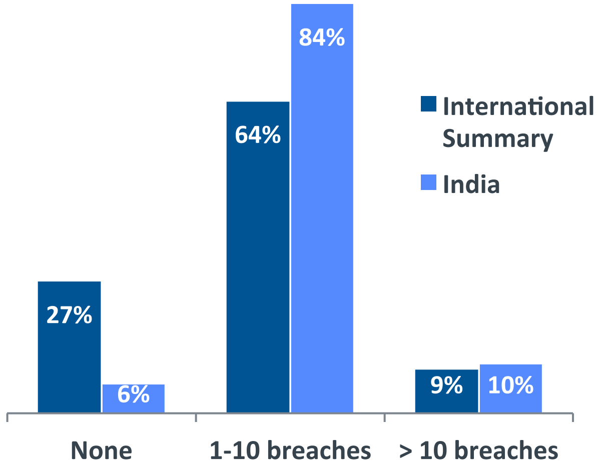
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Roughly four out of five businesses in India expect IT security to grow in importance (84% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In India, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

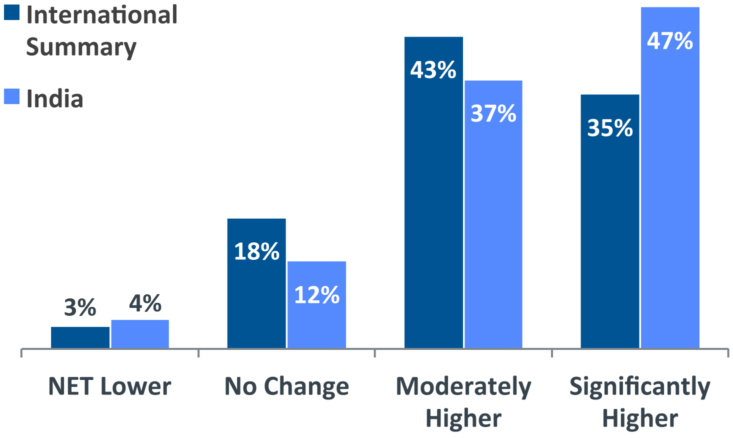
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



84%
NET of **India** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among India businesses

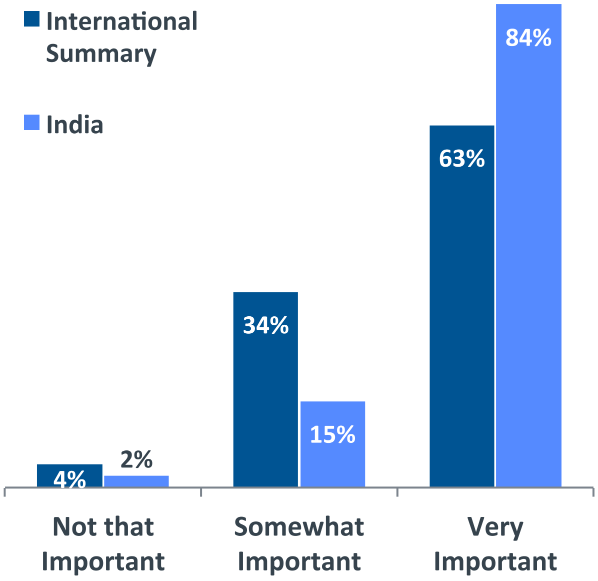
1. Change in IT operations (e.g. cloud, mobility)
2. Internal security breach or incident
3. Change in business operations or client base
4. Reports of security breaches at other firms
5. Knowledge gained from training/certification

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

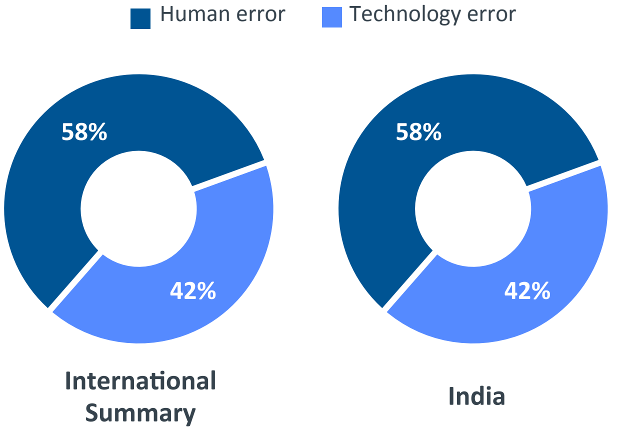
While 94% of India organizations experienced at least one security incident, 9 in 10 also reported one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In India, it is more of a factor now vs. two years ago for nearly three-quarters (72% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 99% in India). And most managers believe it is important to test after IT security training to confirm knowledge gains (98% net very important + somewhat important in India). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Nine in ten managers in India indicate that IT security certifications are very valuable (50%) or valuable (41%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among India businesses

1. Lack of expertise with websites and applications
2. Lack of expertise with networks, servers and other infrastructure
3. Failure to get up to speed on new threats
4. IT staff failure to follow policies and procedures
5. End user failure to follow policies and procedures
6. General carelessness

92%

% of **India** businesses reporting a mobile related security incident. Top issues: lost device, mobile malware, and data policy violation.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Japan

April 2016

EXECUTIVE SUMMARY

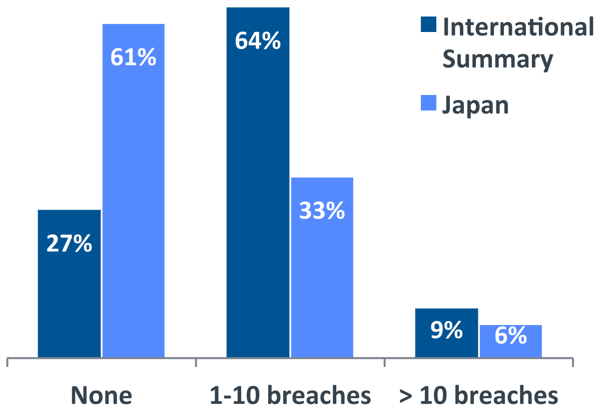
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly two-thirds of businesses in Japan expect IT security to grow in importance (64% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Japan, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

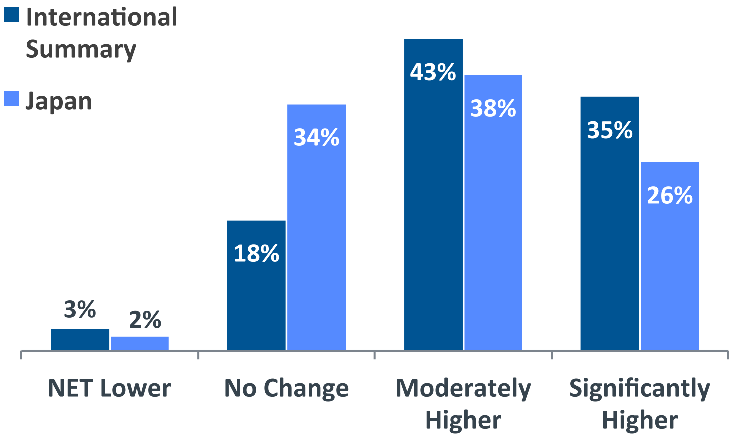
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



64%
NET of **Japan** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Japan businesses

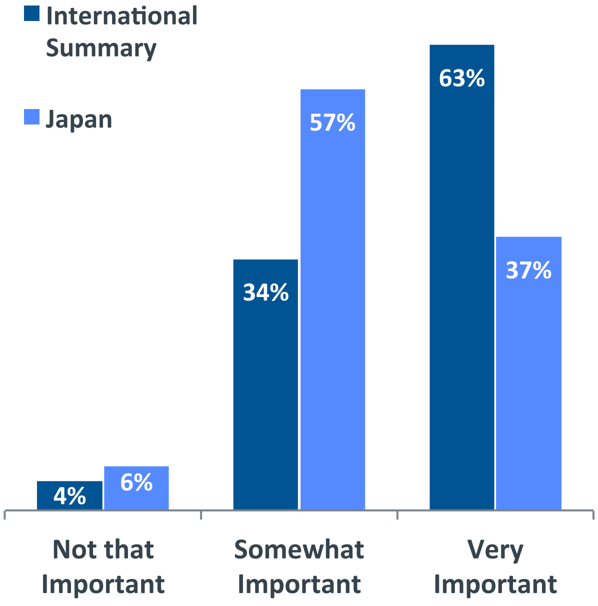
1. Change in IT operations (e.g. cloud, mobility)
2. Internal security breach or incident
3. Reports of security breaches at other firms
4. Vulnerability discovered by an outside party
5. Knowledge gained from training /certification

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

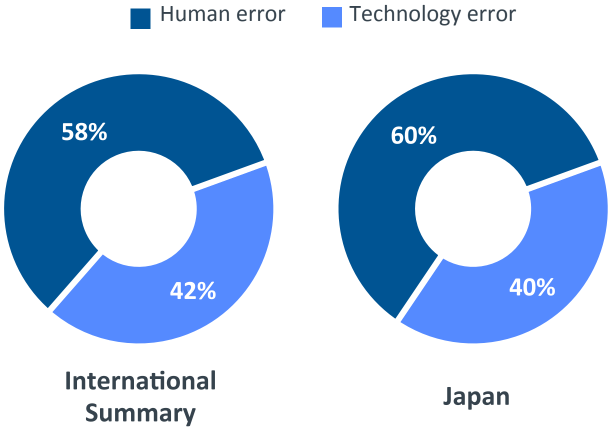
While 4 in 10 Japan organizations experienced at least one security incident, slightly over a fifth had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Japan, it is more of a factor now vs. two years ago for more than half (59% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 86% in Japan). And most managers believe it is important to test after IT security training to confirm knowledge gains (94% net very important + somewhat important in Japan). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Nearly two-thirds of managers in Japan indicate that IT security certifications are very valuable (13%) or valuable (47%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Japan businesses

1. General carelessness
2. Failure to get up to speed on new threats
3. Intentional disabling of security features
4. Inadequate resources/lack of time to manage threats
5. Lack of expertise with networks, servers and other infrastructure
6. End user failure to follow policies and procedures

60%

% of **Japan** businesses reporting a mobile related security incident. Top issues: lost device, data policy violation, and mobile phishing attacks.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Malaysia

April 2016

EXECUTIVE SUMMARY

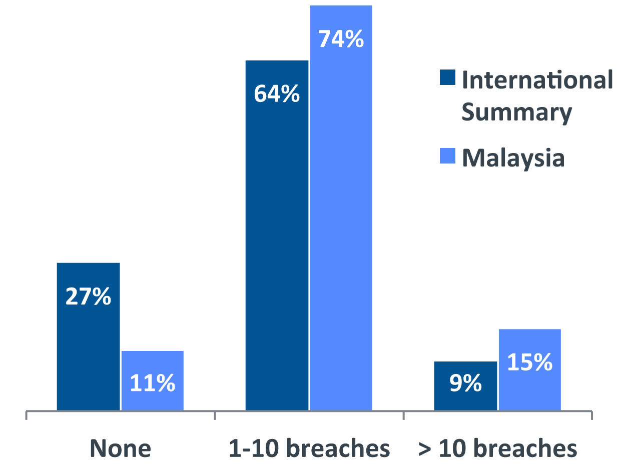
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Slightly over 9 in 10 businesses in Malaysia expect IT security to grow in importance (92% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Malaysia, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

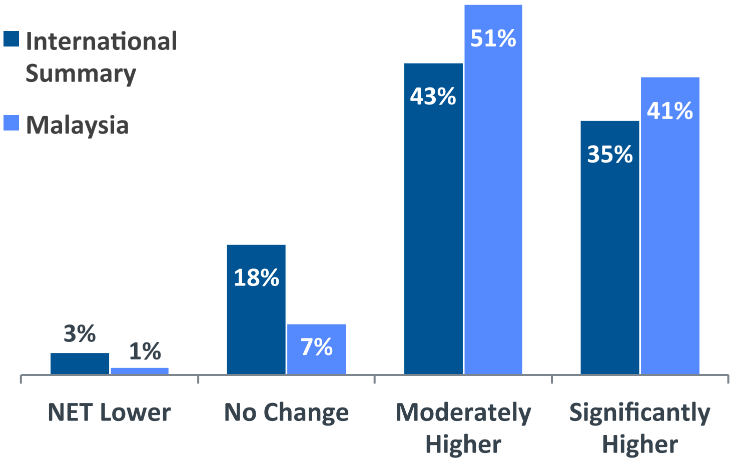
Over the past 12 months

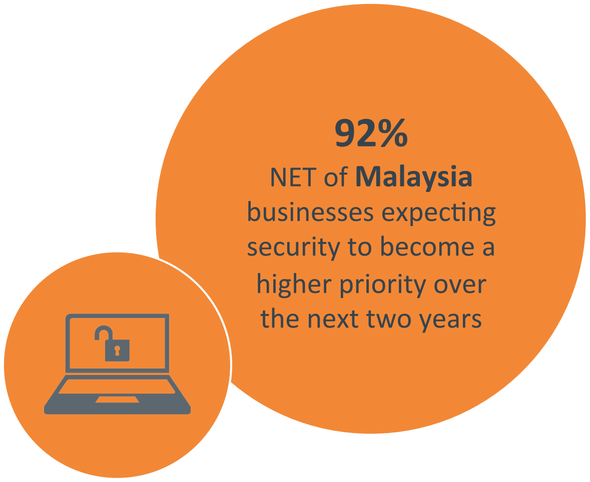


*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today





92%
NET of **Malaysia** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Malaysia businesses

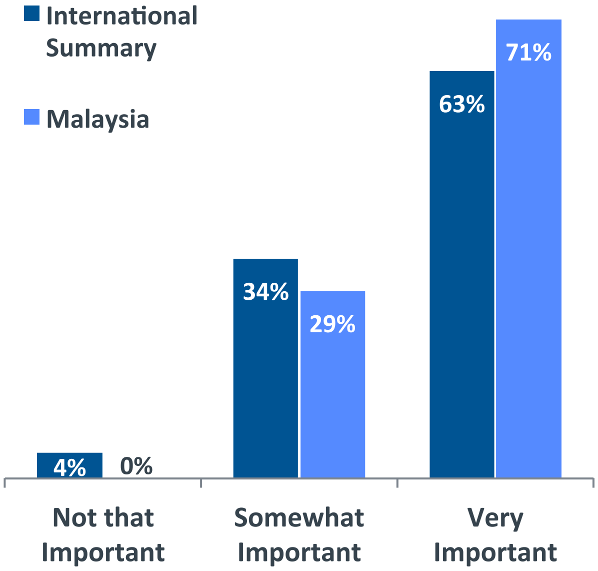
1. Change in IT operations (e.g. cloud, mobility)
2. Internal security breach or incident
3. Knowledge gained from training/certification
4. Reports of security breaches at other firms
5. Change in management

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

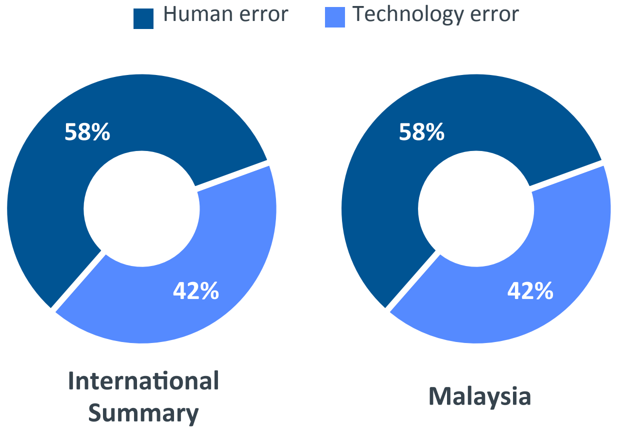
While 9 in 10 organizations in Malaysia experienced at least one security incident, 8 in 10 had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Malaysia, it is more of a factor now vs. two years ago for about three-quarters (74% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 98% in Malaysia). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (100% net very important + somewhat important in Malaysia). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Most managers in Malaysia indicate that IT security certifications are very valuable (41%) or valuable (48%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Malaysia businesses

1. General carelessness
2. Lack of expertise with networks, servers and other infrastructure
3. Lack of expertise with websites and applications
4. IT staff failure to follow policies and procedures
5. End user failure to follow policies and procedures
6. Inadequate resources/lack of time to manage threats

80%
% of **Malaysia** firms reporting a mobile related security incident. Top issues: mobile phishing attacks, lost device, and staff disabling security features.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Mexico

April 2016

EXECUTIVE SUMMARY

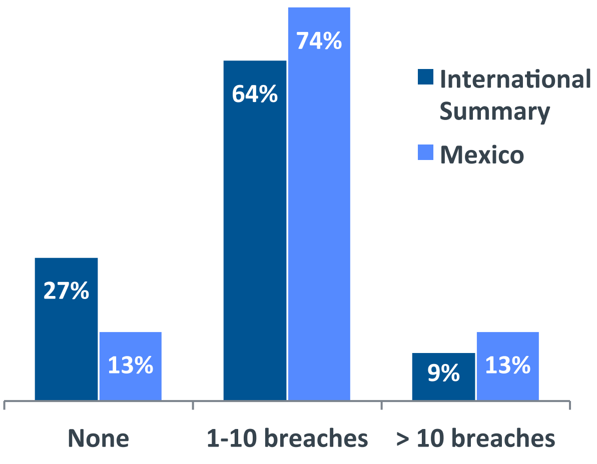
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). More than three-quarters of businesses in Mexico expect IT security to grow in importance (78% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Mexico, similar to many of the other countries, one of the greatest factors has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another notable driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

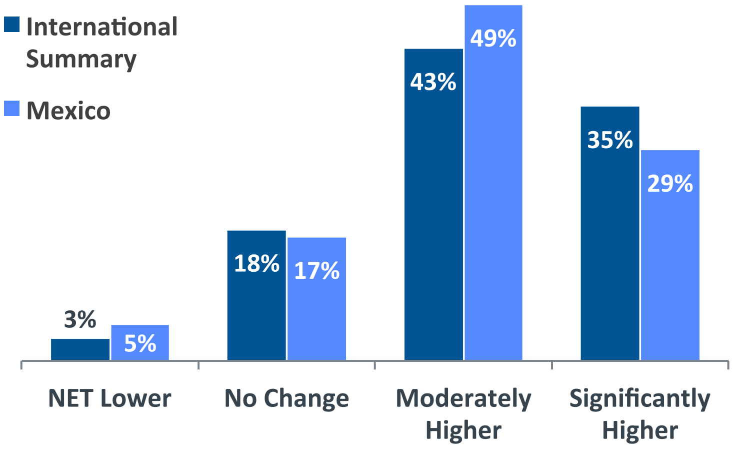
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



78%
NET of **Mexico** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Mexico businesses

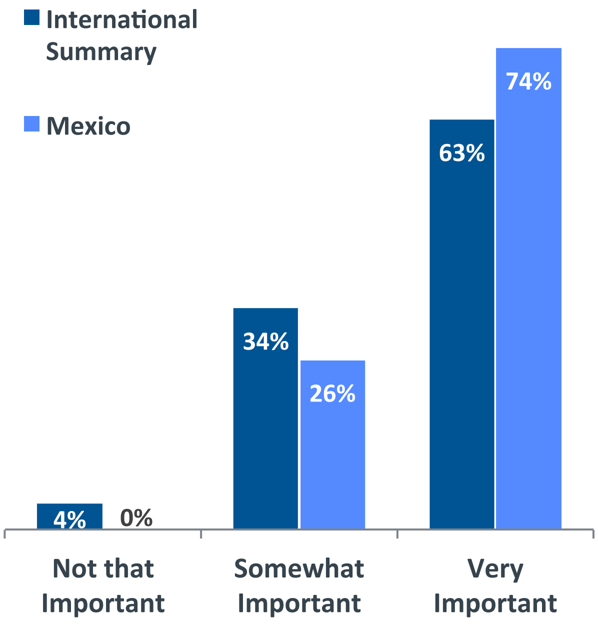
1. Vulnerability discovered by an outside party
2. Change in IT operations (e.g. cloud, mobility)
3. Change in management
4. Knowledge gained from training/certification
5. Focus on a new industry vertical

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

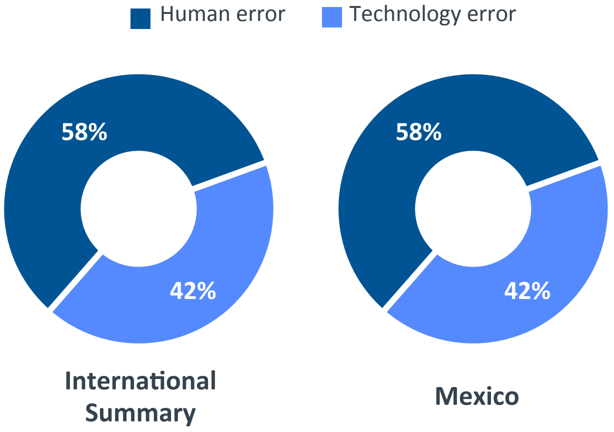
While nearly 9 in 10 Mexico organizations experienced at least one security incident, nearly three-quarters had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Mexico, it is more of a factor now vs. two years ago for nearly more than two-thirds of businesses (69% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 98% in Mexico). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (100% net very important + somewhat important in Mexico). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Most managers in Mexico indicate that IT security certifications are very valuable (45%) or valuable (52%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Mexico businesses

1. Lack of expertise with websites and applications
2. IT staff failure to follow policies and procedures
3. Failure to get up to speed on new threats
4. General carelessness
5. Lack of expertise with networks, servers and other infrastructure
6. End user failure to follow policies and procedures

89%
% of **Mexico** businesses reporting a mobile related security incident. Top issues: lost device, mobile malware, and staff disabling security features.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for South Africa

April 2016

EXECUTIVE SUMMARY

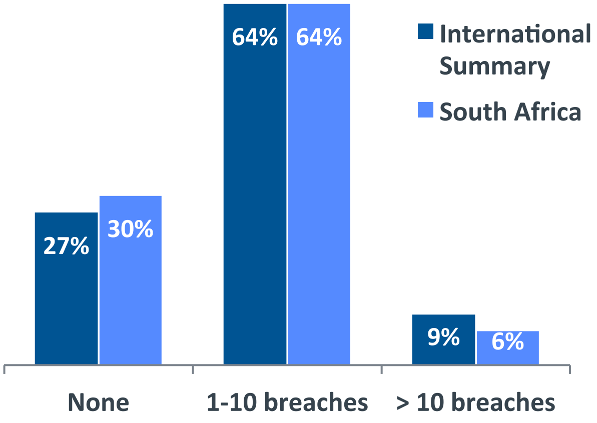
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Slightly over 9 in 10 businesses in South Africa expect IT security to grow in importance (93% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In South Africa, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

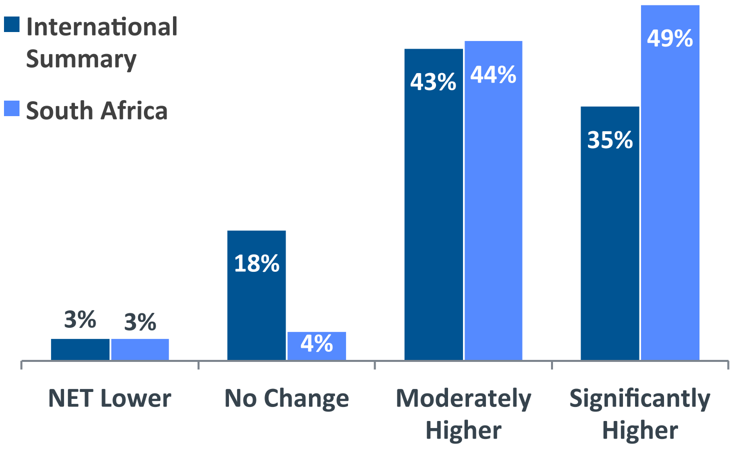
Over the past 12 months

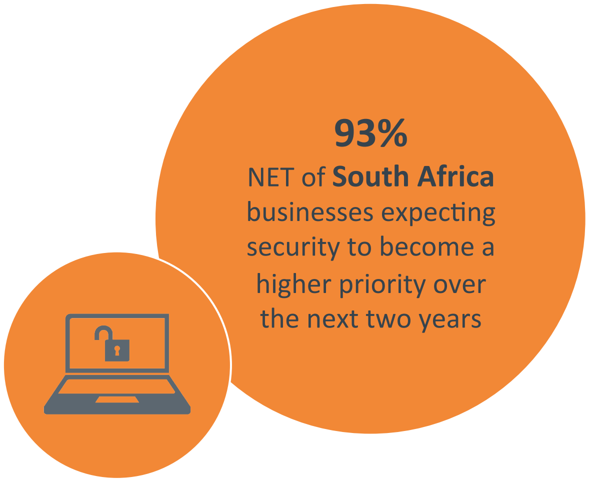


*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today





93%
NET of **South Africa** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among South Africa businesses

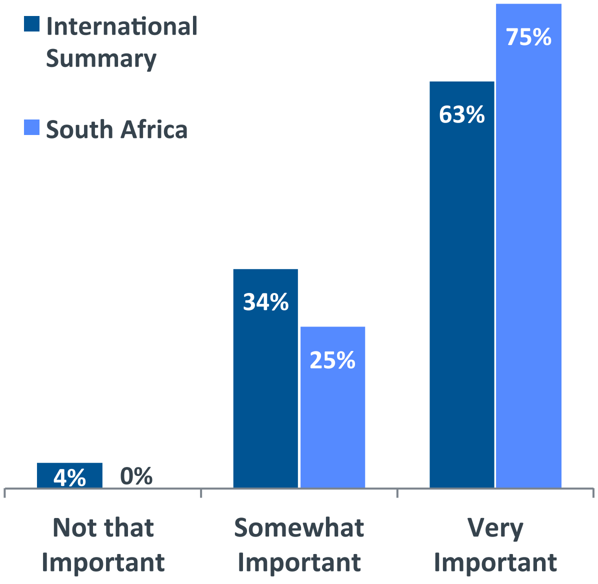
1. Change in IT operations (e.g. cloud, mobility)
2. Reports of security breaches at other firms
3. Knowledge gained from training/certification
4. Change in business operations or client base
5. Internal security breach or incident

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

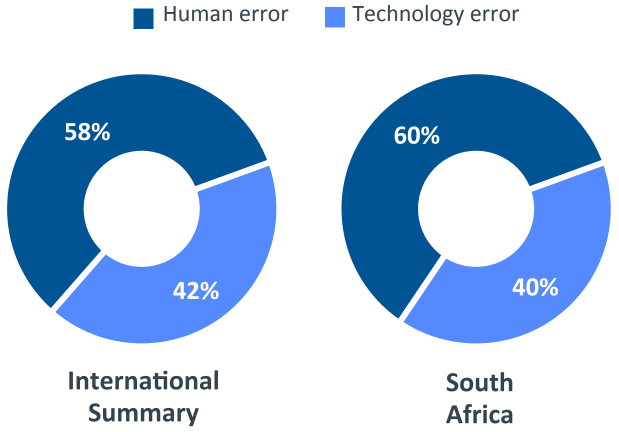
While 7 in 10 organizations in South Africa experienced at least one security incident, slightly over 6 in 10 had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In South Africa, it is more of a factor now vs. two years ago for more than half (58% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 93% in South Africa). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (100% net very important + somewhat important in South Africa). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Most managers in South Africa indicate that IT security certifications are very valuable (49%) or valuable (36%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among South Africa businesses

1. General carelessness
2. Failure to get up to speed on new threats
3. Lack of expertise with websites and applications
4. End user failure to follow policies and procedures
5. IT staff failure to follow policies and procedures
6. Lack of expertise with networks, servers and other infrastructure

77%

% of **South Africa** firms reporting a mobile related security incident. Top issues: lost device, staff disabling security features, and data policy violation.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for Thailand

April 2016

EXECUTIVE SUMMARY

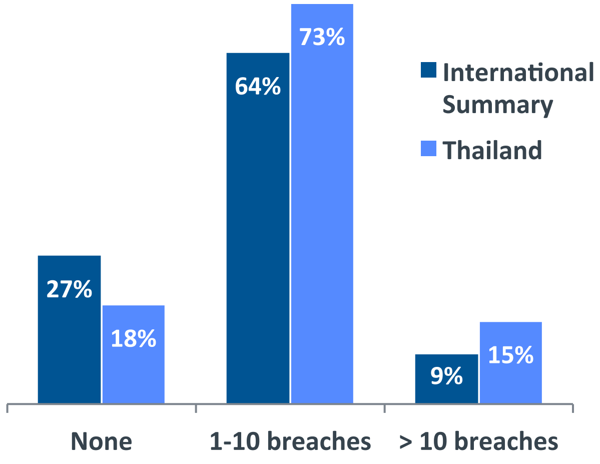
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly 9 in 10 businesses in Thailand expect IT security to grow in importance (89% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In Thailand, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

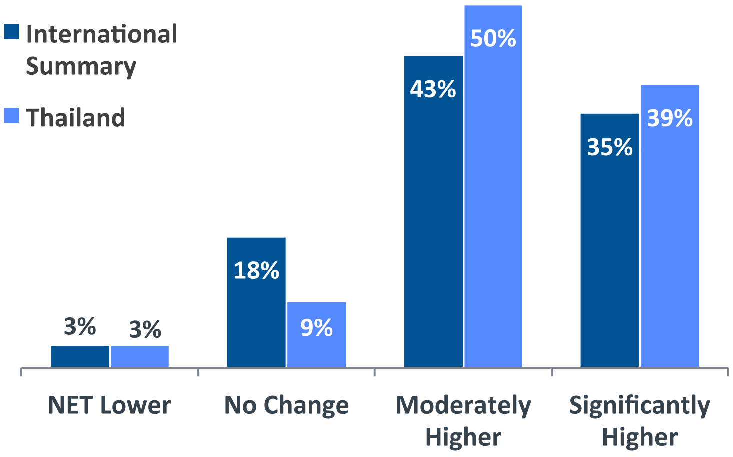
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



89%
NET of **Thailand** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among Thailand businesses

1. Change in IT operations (e.g. cloud, mobility)
2. Change in management
3. Change in business operations or client base
4. Internal security breach or incident
5. Vulnerability discovered by an outside party

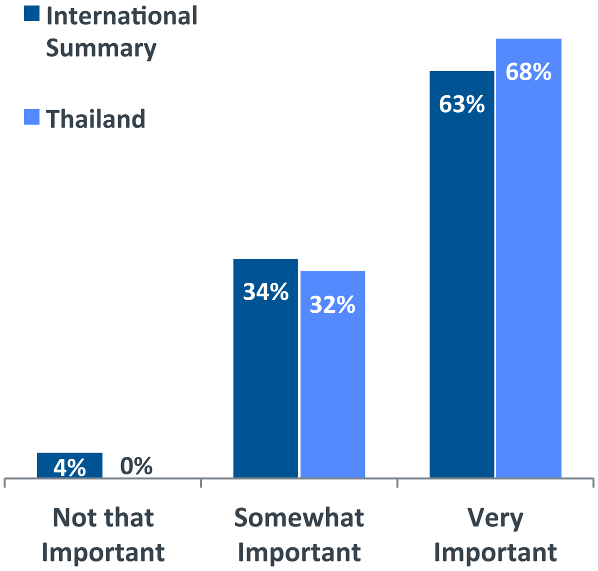
Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

CompTIA.

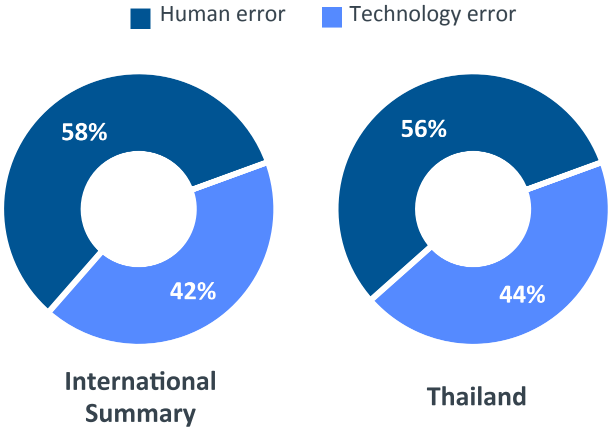
While slightly over 8 in 10 organizations in Thailand experienced at least one security incident, nearly three-quarters had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In Thailand, it is more of a factor now vs. two years ago for about three-quarters (77% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 97% in Thailand). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (100% net very important + somewhat important in Thailand). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). More than 9 in 10 managers in Thailand indicate that IT security certifications are very valuable (42%) or valuable (51%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among Thailand businesses

1. General carelessness
2. Lack of expertise with networks, servers and other infrastructure
3. Lack of expertise with websites and applications
4. End user failure to follow policies and procedures
5. Failure to get up to speed on new threats
6. IT staff failure to follow policies and procedures

95%
% of **Thailand** firms reporting a mobile related security incident. Top issues: mobile malware, mobile phishing attacks, and data policy violation.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for the United Arab Emirates

April 2016

EXECUTIVE SUMMARY

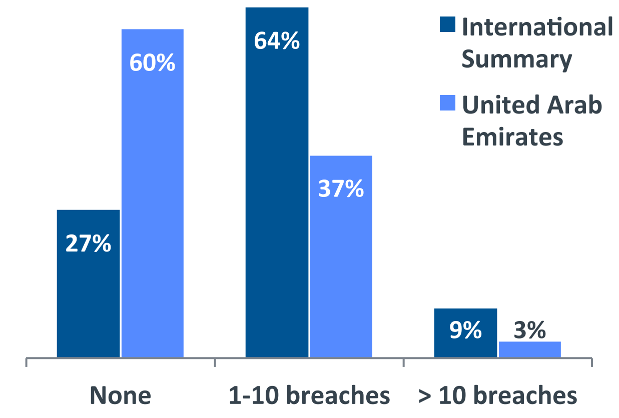
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly 8 in 10 businesses in the United Arab Emirates (UAE) expect IT security to grow in importance (79% net higher).

Due to the evolving nature of IT, the great majority of organizations have had to respond by changing the way their company approaches security. In most of the countries surveyed, one of the greatest factors has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is reports of security breaches at other firms. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

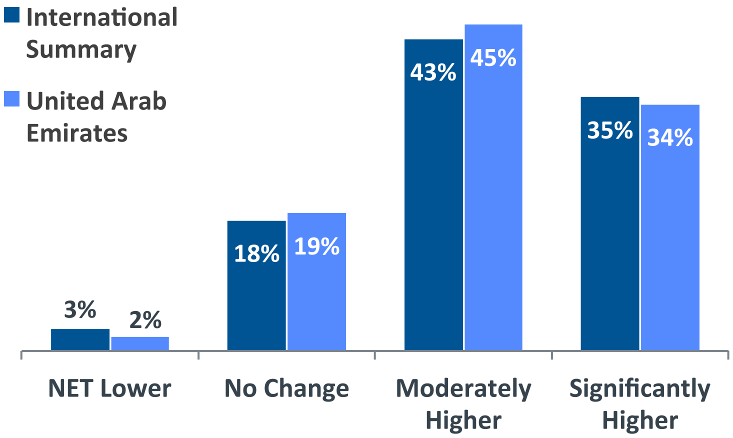
Over the past 12 months

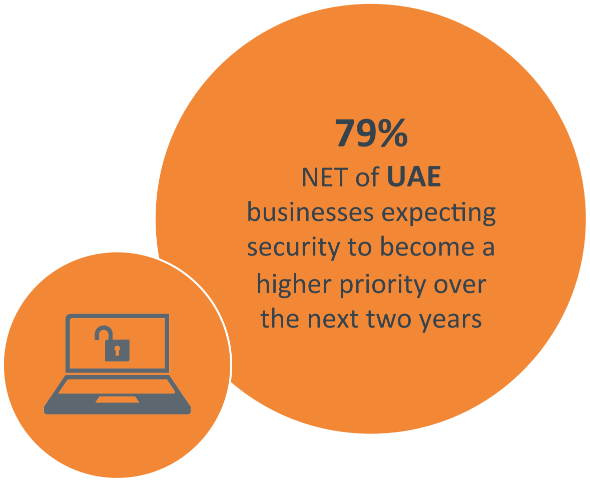


*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today





79%
NET of **UAE** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among UAE businesses

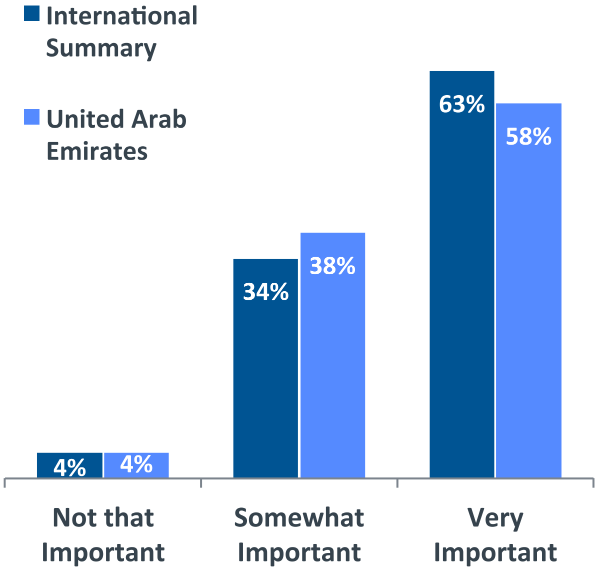
1. Reports of security breaches at other firms
2. Change in management
3. Change in business operations or client base
4. Focus on a new industry vertical
5. Knowledge gained from training/certification
6. Change in IT operations (e.g. cloud, mobility)

Note: see the last page for which countries are categorized in Maturing Economies vs. Mature Economies.

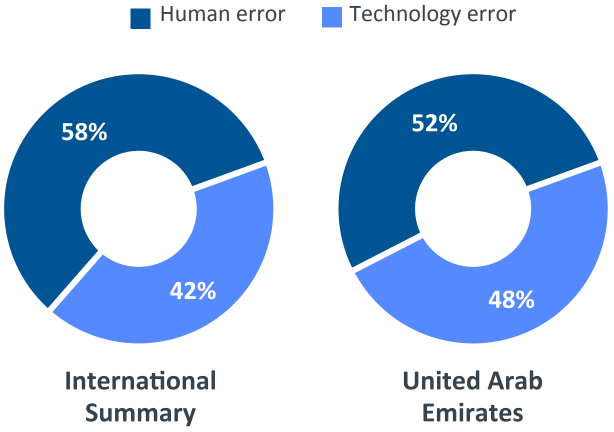
While 4 in 10 organizations in the UAE experienced at least one security incident, about 3 in 10 had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In the UAE, it is more of a factor now vs. two years ago for more than a third (39% net human error more of a factor).

On the brighter side, the majority of firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 79% in the UAE). And nearly all managers believe it is important to test after IT security training to confirm knowledge gains (96% net very important + somewhat important overall as well as in the UAE). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Three-quarters of managers in the UAE indicate that IT security certifications are very valuable (43%) or valuable (32%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among UAE businesses

1. End user failure to follow policies and procedures
2. General carelessness
3. Lack of expertise with networks, servers and other infrastructure
4. Lack of expertise with websites and applications
5. Intentional disabling of security features
6. Failure to get up to speed on new threats

60%
% of **UAE** firms reporting a mobile related security incident. Top issues: mobile phishing attacks, lost device, staff disabling security features, and data policy violation.

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for the United Kingdom

April 2016

EXECUTIVE SUMMARY

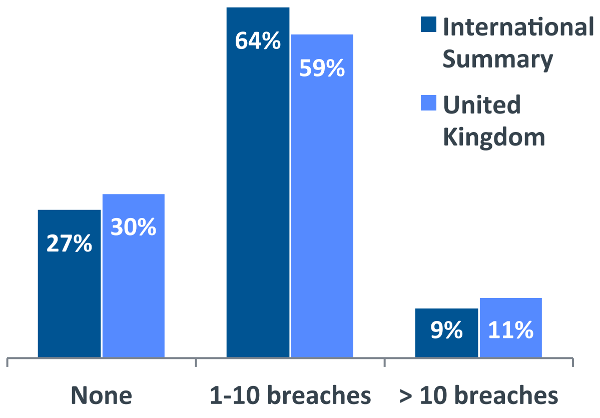
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly two-thirds of businesses in the United Kingdom (UK) expect IT security to grow in importance (66% net higher).

Due to the evolving nature of IT, the great majority of organisations have had to respond by changing the way their company approaches security. In the UK, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/ incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

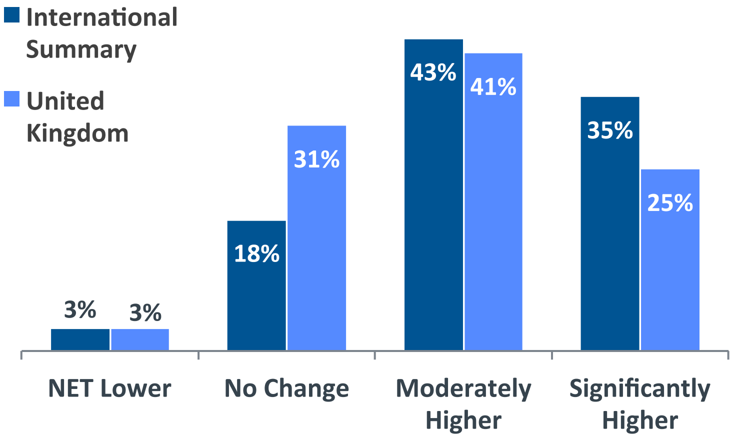
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



66%

NET of **UK** businesses expecting security to become a higher priority over the next two years

TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among UK businesses

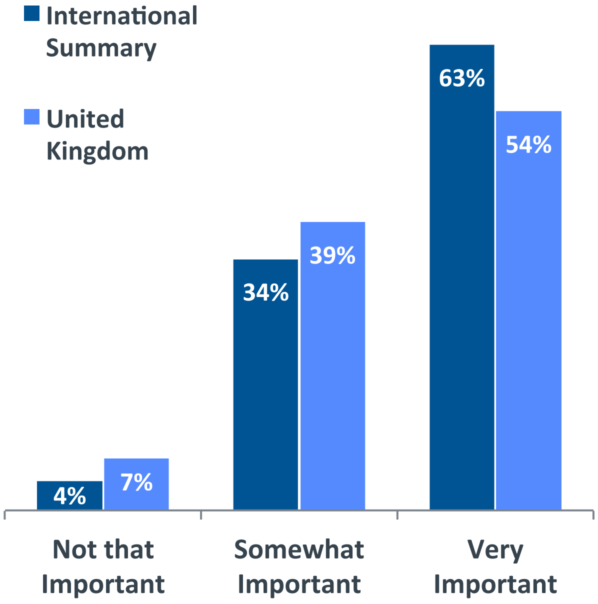
1. Change in IT operations (e.g. cloud, mobility)
2. Internal security breach or incident
3. Change in business operations or client base
4. Reports of security breaches at other firms
5. Change in management

Note: see the last page for which countries are categorised in Maturing Economies vs. Mature Economies.

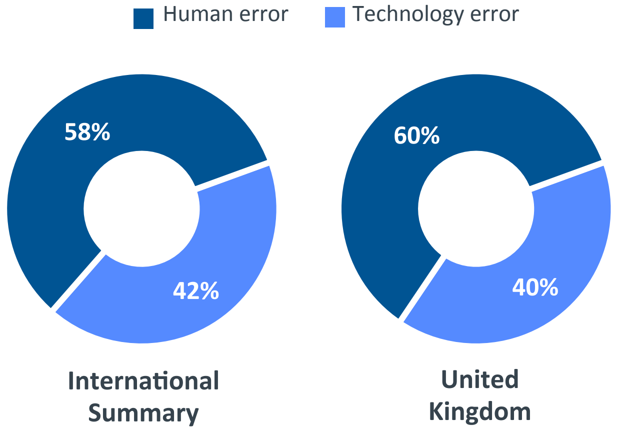
While 7 in 10 UK organisations experienced at least one security incident, slightly over half had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In the UK, it is more of a factor now vs. two years ago for more than half (56% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 90% in the UK). And most managers believe it is important to test after IT security training to confirm knowledge gains (93% net very important + somewhat important in the UK). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Nearly two-thirds of UK managers indicate that IT security certifications are very valuable (33%) or valuable (32%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among UK businesses

1. General carelessness
2. IT staff failure to follow policies and procedures
3. End user failure to follow policies and procedures
4. Lack of expertise with networks, servers and other infrastructure
5. Lack of expertise with websites and applications
6. Failure to get up to speed on new threats

64%
% of **UK** businesses reporting a mobile related security incident. Top issues: lost device, data policy violation, mobile malware, and mobile phishing attacks.

RESEARCH METHODOLOGY

CompTIA's *International Trends in Cybersecurity* was conducted to collect and share quantitative information on behaviors, techniques, and opportunities associated with IT security across 12 countries. More information and all country snapshots are available at CompTIA.org/internationalsecurity.

A total of 1,509 IT and business executives participated in the online survey during January – February 2016, yielding an overall margin of sampling error at 95% confidence of +/- 2.5 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is a member of the Marketing Research Association and abides by its guidelines for survey best practices and research ethics.

CompTIA is responsible for all content contained in this report. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

Job Role

22%	Executive Mgt. (CEO, President, Owner, etc.)
23%	Senior Mgt. – IT function (CIO, CSO, VP, etc.)
10%	Middle Mgt. – IT function (Director, Team Lead)
11%	Staff level – IT function
21%	Senior Mgt. – Business function (CFO, VP, etc.)
6%	Middle Mgt. – Business (Director, Team Lead)
8%	IT Consultant

SURVEY DEMOGRAPHICS

Firm Size

5%	Micro firm (5 to 9 employees)
34%	Small firm (10 to 99 employees)
30%	Medium firm (100 to 499 employees)
30%	Large firm (500 or more employees)

Primary Industry

20%	Information Technology (IT)
14%	Manufacturing (other than IT related)
11%	Professional services (other than IT related)
10%	Retail/Wholesale (other than IT related)
6%	Healthcare/Medical
8%	Financial/Banking/Insurance
2%	Media/Publishing/Entertainment
3%	Government (federal, state, local)
7%	AMTUC (Agriculture, Mining, Transportation, Utilities, Construction)
6%	Education
3%	Hospitality
9%	Other industry

Countries

n	Maturing Economies	n	Mature Economies
126	Brazil	125	Australia
131	India	125	Canada
125	Malaysia	125	Germany
126	Mexico	125	Japan
125	South Africa	125	UK
125	Thailand		
126	UAE		
884	Total Maturing	625	Total Mature
1,509	Total number of respondents in the study		

ABOUT COMPTIA

CompTIA is the voice of the world's information technology (IT) industry and workforce.

Its members are the companies at the forefront of innovation; and the professionals responsible for maximizing the benefits organizations receive from their investments in technology.

CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications, and public policy advocacy.