Where are organizations investing their IT security dollars, and just how confident are they in their ability to protect data from a variety of intrusions? Gemalto set out to answer these key questions in a new research report entitled “Data Security Confidence Index.”

The study, based on research conducted by Vanson Bourne on behalf of Gemalto, queried more than 1,000 security and IT executives in the U.S., UK, Europe, Middle East and Asia-Pacific.

The survey respondents included executives from a variety of industries including financial services, healthcare, manufacturing, public sector, telecommunications, utilities, retail, construction, insurance, legal and others.

In conducting the research, Gemalto was aiming to find out not only the level of confidence among organizations with regard to information security, but also whether their security strategies were actually in sync with their data protection needs and the threats and vulnerabilities that are predominant today.

By gaining insights into the confidence levels of companies as well as how they are spending their security budgets, the research will provide guidelines for enterprises looking to make significant improvements in their information security posture.
Global Key Findings

Over half (53%) of respondents’ organizations use a combination of internal and external perimeter security systems.

Around eight in ten respondents’ organizations utilize perimeter security (82%) and/or data security (80%).

More respondents’ organizations are going to increase their perimeter security investments over the next twelve months, up from 57% in 2014 to 72% in 2015.

Nearly two in five (38%) respondents’ organizations plan to expand into a form of perimeter security systems not currently being used.

Over the next twelve months almost two thirds (64%) plan to increase their investment in current or planned perimeter security systems.

The security budgets allocated to perimeter security technology has and will remain constant at around 9%.

The majority (73%) of respondents think that their organization invests enough in security and over four in five (83%) think that their organization invests in the right technologies.

87%

The majority (87%) of respondents believe that their organizations’ perimeter security systems are effective at keeping unauthorized users out of their network.

Around a third think unauthorized users are able to access their organizations’ network (33%) and are not confident that their organizations’ data would be secure if unauthorized users penetrated their network perimeter (34%).

30%

There has been an increase in breaches over the last 12 months with 30% of respondents’ organizations reporting that they have been breached.

In three quarters (75%) of respondents’ organizations’ most recent breaches, one or more of the sources has been external compared to just over half (54%) where one or more of the sources is internal.

Nine in ten (90%) respondents’ organizations suffered negative commercial consequences as a result of being breached.

A delay in product/service development (31%) is the most common consequence.

Other consequences include a decrease in employee productivity (30%), decreased customer confidence (28%) and negative press (24%).

More budget (75%), resources (55%) and time (61%) is spent on protecting customer data over protecting their organizations’ intellectual property.

Almost a quarter (24%) of respondents admit that they do not feel their organization has the security capabilities necessary to keep up with emerging threats and technologies.

One in every six (15%) IT decision makers surveyed would not trust their own organization to manage and store their personal data.

Around three out of five (62%) respondents are no more confident than they were this time last year in the security industry’s ability to detect and defend against emerging security threats.

High-profile data breaches have driven over seven in ten (71%) respondents’ organizations to adjust their security strategy.
900 IT decision makers were interviewed in February 2015, split in the following ways.

Country
- US: 200
- UK: 100
- France: 100
- Germany: 100
- Poland: 100
- Benelux: 50
- Czech Republic: 50
- Middle East: 50
- Hong Kong: 50
- Japan: 50
- Australia: 50

Sector
- Manufacturing: 145
- Financial Services: 128
- Telecommunications: 127
- Healthcare: 115
- Retail: 111
- Government: 93
- Other Sector: 66
- Utilities: 43
- Construction & Real Estate: 41
- Insurance & Legal: 31

Organization size
- 100-250 Employees: 183
- 251-500 Employees: 196
- 501-1000 Employees: 230
- 1001-5000 Employees: 217
- More than 5000 Employees: 74

900 IT decision makers were interviewed in February 2015, split in the following ways.
Perimeter security investment

Systems utilized in organization’s infrastructure

Over half (53%) of respondents say that their organization uses a combination of internal and external perimeter security systems as part of its IT infrastructure (Fig 1).

Around eight in ten respondents’ organizations utilize perimeter security (82%) and data security (80%) (Fig 2).

This suggests that organizations still widely use perimeter security within their organization.

Fig 1

“Does your organization use internal (software based) perimeter security systems (firewall, IDPS, AV, content filtering, etc.) or an external (hardware based) solution as part of its IT infrastructure?”, asked to all respondents (900 respondents).

Fig 2

“Which of the following do you utilize within your organization?”, asked to all respondents (900 respondents).
Perimeter security investment

Close to three quarters (72%) of respondents say that their organization’s investment in perimeter security systems has increased over the past five years, with only the minority (8%) seeing a decrease in investment.

When compared to the 2014 study, over the last year more respondents’ organizations have increased their perimeter security investments than reported doing so in 2014.

Fig 3
"Over the past five years, how has your investment in perimeter security technology changed?”, asked to all respondents in 2015 (900 respondents).

Fig 4
"Over the past five years, how has your investment in firewall technology changed?”, asked to all respondents in 2014 (1011 respondents).
How investment in perimeter security has changed

90% of respondents’ organizations have increased perimeter security investment over the past five years.

78% say that their organization has increased investment in data security, and 74% say they have increased investment in identity and access control.

The increased investment aligns with the technology most utilized in respondents’ organizations (Fig 1 and 2) therefore the level of increased investment within these forms of perimeter security is not surprising.

Fig 5

"How has your investment in perimeter security technology changed over the past five years?", asked to all respondents (900 respondents).

<table>
<thead>
<tr>
<th>Perimeter Security</th>
<th>90%</th>
</tr>
</thead>
<tbody>
<tr>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>7%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>78%</td>
</tr>
<tr>
<td>7%</td>
</tr>
<tr>
<td>15%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity &amp; Access Control</th>
<th>74%</th>
</tr>
</thead>
<tbody>
<tr>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>9%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increased</th>
<th>Stayed the same</th>
<th>Decreased</th>
</tr>
</thead>
<tbody>
<tr>
<td>90%</td>
<td>4%</td>
<td>7%</td>
</tr>
</tbody>
</table>
Security budget spend

9% of respondents’ organizations’ security budget is spent on purchasing, deploying and maintaining perimeter security systems on average.

Similarly respondents’ organizations spent 9% of their security budget in the 2014 study.

Although budgets often get squeezed, respondents’ organizations have kept the amount allocated to perimeter security at a constant level over the past two years highlighting the importance of these systems.

Fig 6
Analysis on how much of respondents’ organizations’ security budget is spent on purchasing, deploying and maintaining perimeter security technology.

- Average percentage of security budget spent on perimeter security in 2015: 9.00%
- Average percentage of security budget spent on firewall technology in 2014: 8.54%
Perimeter security investment

Future perimeter security investment

Around **two in five 38%** respondents’ organizations plan to expand into a form of perimeter security systems not currently in use (fig 7).

Over the next twelve months, around **two thirds 64%** of respondents’ organizations plan to increase investment in current or planned perimeter security systems (fig 8).

This shows respondents’ organizations are looking to further increase their investment in perimeter security.

---

**Fig 7**

Analysis on respondents’ organizations’ plans to invest, over the next 12 months, into a form of perimeter security not currently being used, asked to all respondents (900 respondents).

<table>
<thead>
<tr>
<th>Will invest in a form of perimeter security technology not currently in use in the next 12 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>62%</td>
</tr>
<tr>
<td>38%</td>
</tr>
</tbody>
</table>

**Fig 8**

Analysis on how respondents’ organizations’ investment in perimeter security technology will change over the next 12 months, asked to all respondents for current or planned perimeter security.

<table>
<thead>
<tr>
<th>Perimeter Security</th>
<th>Data Security</th>
<th>Identity &amp; Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>6%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>30%</td>
<td>31%</td>
<td>36%</td>
</tr>
<tr>
<td>64%</td>
<td>58%</td>
<td>53%</td>
</tr>
</tbody>
</table>

- Increased
- Stayed the same
- Decreased
Are organizations investing enough?

**Fig 9**
Analysis on respondents’ views on organizations’ investment in security, asked to all respondents.

- **Do you think your organisation invests enough in security?**
  - [900 respondents in 2015]
  - 73% Yes, 27% No

- **Do you think your organisation invests enough in security?**
  - [1003 respondents in 2014]
  - 50% Yes, 50% No

**Fig 10**
Analysis on respondents’ views on organizations’ investment into the right security technologies, asked to all respondents.

- **Do you think your organisation investments in security go to the right technologies?**
  - [900 respondents in 2015]
  - 83% Yes, 17% No

- **Do you think your organisation investments in security go to the right technologies?**
  - [1005 respondents in 2014]
  - 71% Yes, 29% No

The majority **73%** of respondents think their organization invests enough in security (Fig 9) and over **four in five 83%** think that their organization invests in the right technologies (Fig 10).

Could the increased investments made by respondents’ organizations over the past five years (fig 3 and 4) be leading them to believe they are investing enough and to the right technologies?
Allocating security budget spend

Were the respondent to be in charge of their organization’s security budget, nearly half (48%) would allocate the most spend to data security and a third (32%) would allocate the most to perimeter security (fig 11).

Only a small minority (6%) would allocate the most spend to anomaly detection (fig 11). Respondents would be more than twice as likely to get rid of this technology (36%) than perimeter security (16%) (fig 12).

This suggests that perimeter security is considered important by most IT decision makers.
Perimeter security systems effectiveness

The majority (87%) of respondents feel that their organizations’ perimeter security systems are effective at keeping out unauthorized users.

This belief has increased since 2014 (74%) and is no surprise given the increase in respondents’ organizations investment over the last year (Fig 3 and 4).

This increased belief along with respondents feeling they are investing enough and to the right technologies (Fig 9 and 10) give reason to why respondents believe their organizations’ security systems are effective at keeping out unauthorized users.

But does perception align with reality?

Fig 13
“How effective do you feel perimeter security systems are at keeping unauthorized users out of your network?”, asked to all respondents (900 respondents).
The reality: organizations’ breaches

Unauthorized users gaining access to the network

A third (33%) of respondents’ organizations think that unauthorized users are able to access their organization’s network.

A similar number (34%) are not confident that their organizations’ data would be secure if unauthorized users penetrated their network perimeter.

Respondents’ confidence was higher in 2014 which shows the increased investment in perimeter security technology has not lead to greater confidence in security.

This suggests that despite heavy investment in perimeter security technology and confidence in current systems, there is room for improvement.

Have perimeter security breaches increased over the past twelve months?

Fig 14
Analysis if unauthorized users can access respondents’ organizations’ network and if organization’s data would still be secure if this were to happen, asked to all respondents.

- Respondents in 2015 that think unauthorised users could access organisation’s network [900]
- Respondents in 2014 that think unauthorised users could access organisation’s network [1014]
- Respondents in 2015 not confident organisation’s data would be secure if unauthorised users accessed network [900]
- Respondents in 2014 not confident organisation’s data would be secure if unauthorised users accessed network [1014]
The reality: organizations’ breaches

**Perimeter security system breaches**

There has been an increase in breaches over the last 12 months with 30% of respondents’ organizations reporting that they have been breached (Fig 15).

This year more respondents report that their organizations’ perimeter security systems have been breached compared to 2014 (Fig 16), despite the fact that fewer respondents feel unauthorized users can access their organizations’ network, now than in 2014 (Fig 14), is this a false sense of security?

**Fig 15**

“Has your organization’s perimeter security system been breached?”, asked to all respondents (900 respondents).

- In the past 12 months: 30%
- More than 12 months but less than 18 months: 24%
- More than 18 months but less than 24 months: 26%
- More than 24 months ago: 32%

**Fig 16**

Analysis comparing respondents’ organizations that have been breached in 2015 and 2014.

- Yes at any timeframe in 2015 [900]: 54%
- Yes in 2014 [1017]: 22%
The reality: organizations’ breaches

Most common breaches experienced

The most common forms of respondents’ organizations’ perimeter security system breaches are viruses (76%) and malware (74%) (Fig 17).

RansomWeb is a relatively new breach and has steadily increased over the last 24 months (Fig 18).

There are various perimeter security system breaches experienced by respondents’ organizations requiring a more effective solution to protect against them. These need to be adaptable to protect against the newer forms of breaches.

Fig 17
"Analysis on respondents’ organizations’ most recent perimeter security breach, asked to respondents whose organization experienced a breach (499 respondents).

<table>
<thead>
<tr>
<th>Breach</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>76%</td>
</tr>
<tr>
<td>Malware</td>
<td>74%</td>
</tr>
<tr>
<td>Trojan Horses</td>
<td>66%</td>
</tr>
<tr>
<td>Spyware</td>
<td>60%</td>
</tr>
<tr>
<td>Phishing for passwords</td>
<td>55%</td>
</tr>
<tr>
<td>SQL injection</td>
<td>50%</td>
</tr>
<tr>
<td>DDoS attacks</td>
<td>49%</td>
</tr>
<tr>
<td>Botnets</td>
<td>46%</td>
</tr>
<tr>
<td>RansomWeb</td>
<td>46%</td>
</tr>
<tr>
<td>Suspected or known AETs</td>
<td>43%</td>
</tr>
</tbody>
</table>

Fig 18
Analysis on how RansomWeb attacks have increased over the past 24 months.

- In the past 12 months: 21%
- More than 12 months but less than 18 months: 11%
- More than 18 months but less than 24 months: 12%
- More than 24 months ago: 5%
The reality: organizations’ breaches

Percentage of breached data protected by encryption

When thinking about respondents’ organizations’ most recent breach, the average amount of breached data protected by encryption was 7.77%.

The small percentage of breach data being encrypted highlights the need for a more robust system limiting the amount of unencrypted data being breached.

With the majority (80%) of respondents’ organizations utilising data security, which includes encryption, (Fig 2) and such a small amount of breached data being encrypted this highlights a need for organizations to use the systems they have more effectively.

Fig 19

“Thinking about your organization’s most recent breach, what percentage of the breached data was protected by encryption?”, asked to respondents whose organization experienced a breach (499 respondents).

- 0%: 4%
- 1%: 4%
- 2%: 15%
- 3%: 19%
- 4%: 20%
- 5-10%: 24%
- More than 10%: 7%
- Don’t know: 7%
The reality: organizations’ breaches

Source of most recent breach

The most common source of perimeter security system breach experienced by respondents’ organizations’ was a malicious outsider 57% while over a third (36%) was from accidental loss.

Three quarters (75%) of all sources of perimeter security breaches experienced by respondents’ organizations were external and just over half (54%) were internal.

This shows that there is a need for security that protects the perimeter both internally and externally.

Fig 20

“What was the source of your most recent breach?”, asked to respondents whose organization experienced a breach (499 respondents)

- Malicious outsider: 57%
- Accidental loss: 36%
- Malicious insider: 32%
- Hacktivist: 21%
- State sponsored: 13%
- Don’t know: 3%

Fig 21

Analysis on respondents’ organizations’ most recent perimeter security system breach being external or internal, asked to respondents whose organization has experienced a breach and know the source of the breach (481 respondents)

- External (Malicious outsider, State sponsored, Hacktivist): 75%
- Internal (Accidental loss, Malicious insider): 54%
- Don’t know: 3%
DSCI RESEARCH RESULTS

The reality: organizations’ breaches

Commercial consequences of breaches

Nine in ten (90%) respondents’ organizations whose perimeter security systems experienced a breach, suffered negative commercial consequences of the breach.

Only 10% report that their organization suffered no commercial consequence.

The most common consequence experienced is a delay in product/service development (31%). However no one consequence is reported by the majority.

This highlights the importance for organizations to protect themselves against breaches and prevent a variety of potential consequences.

Fig 22

Analysis on respondents’ organizations suffering a commercial consequence, asked to respondents whose organization experienced a breach (499 respondents).

Fig 23

“Have any of the following been commercial consequences of the breaches your organization has experienced?”, asked to respondents whose organization experienced a breach (499 respondents).

- Delay in product development: 31%
- Decreased employee productivity: 30%
- Decreased customer confidence: 28%
- Negative press: 24%
- Delayed getting products to market: 23%
- Affected the bottom line: 22%
- Fines/penalties: 20%
- Loss of customers: 18%
- Loss of a new/incremental business: 16%
- Loss of business to a competitor: 11%
- Loss of repeat business: 10%
- Lawsuits/legal action: 8%
Protecting customer data

Security vs. compliance
Respondents report that they worry more about security breaches (85%) than being fined for failing a compliance audit (15%).

This highlights how important respondents regard protecting customer data, leading to an increased need for their organizations to invest into more effective perimeter security.

Is there more emphasis on protecting customer data or the organizations’ intellectual property?

Fig 24
"Which of these would worry you more?", asked to all respondents (900 respondents).

85%
15%

Security breach (e.g. losing customer/employee data)
Being fined for failing a compliance audit
DSCI RESEARCH RESULTS

Protecting customer data vs. organization’s IP

In respondents’ organizations more budget (75%), resources (55%) and time (61%) is spent on protecting customer data than protecting their organizations’ intellectual property.

This shows that respondents’ organizations prioritise protecting customer data over protecting their IP.

Decision makers place great importance on customer data and will look for solutions that protect this type of data from breaches.

With their organizations spending more budget, resource and time on protecting customer data, do respondents feel their organizations have the security capabilities necessary to keep up with emerging threats and technologies?

Fig 25

"Is there more emphasis on protecting customer data (e.g. medical, financial information, personal identifiable information) or protecting your organization’s intellectual property (e.g. embedded devices such as vehicle software, automated machinery etc.)?", asked to all respondents (900 respondents).

More budget is assigned to
- Protecting customer data: 75%
- Protecting the organization’s IP: 25%

More resource is assigned to
- Protecting customer data: 55%
- Protecting the organization’s IP: 45%

More time is spent on
- Protecting customer data: 61%
- Protecting the organization’s IP: 39%
Confidence in organizations’ security capabilities

Almost a quarter (24%) of respondents admit that they do not feel their organization has the security capabilities necessary to keep up with emerging threats and technologies and one in every six (15%) IT decision makers surveyed would not trust their own organization to manage and store their personal data.

This suggests that IT decision makers do not trust their organizations’ perimeter security systems and there is a need for investing into improved more effective solutions.

Despite this, there is an increased feeling in respondents’ organizations’ security capabilities than in 2014.

Respondents have a lack of confidence in their organizations’ security capabilities, is this also true of the security industry as a whole?

Fig 26
Analysis of respondents’ views on organizations’ ability to keep up with emerging threats and technologies and if they would trust organization, as a customer, to store their own personal data, asked to all respondents

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respondents in 2015 that feel organisation does not have security capabilities to keep up with emerging threats</td>
<td>24%</td>
<td>36%</td>
</tr>
<tr>
<td>Respondents in 2014 that feel organisation does not have security capabilities to keep up with emerging threats</td>
<td>15%</td>
<td>25%</td>
</tr>
<tr>
<td>Respondents in 2015 that would not trust organisation to store their personal data</td>
<td>900</td>
<td>1007</td>
</tr>
<tr>
<td>Respondents in 2014 that would not trust organisation to store their personal data</td>
<td>900</td>
<td>1007</td>
</tr>
</tbody>
</table>
Confidence in the security industry

Around three out of five [62%] respondents are no more confident than they were this time last year in the security industry’s ability to detect and defend against emerging security threats [Fig 27].

High-profile data breaches have driven over seven in ten [71%] respondents’ organizations to adjust their security strategy [Fig 28] suggesting that respondents feel a need for their organizations to improve and invest into perimeter security technology to avoid becoming a victim of breaches like the in high-profile cases reported.

With high-profile data breaches reported in the news it is no surprise that there is an increase of respondents’ organizations changing their strategy than in 2014.

Fig 27

“In the past year, have you become more or less confident about the security industry’s ability to detect and defend against emerging security threats?”, asked to all respondents (900 respondents).

Fig 28

“Have the high-profile data breaches in the news driven your organization to adjust its security strategy?”, asked to all respondents.

High-profile data breaches in the news has, to some extent, driven organisation to adjust security strategy [900 respondents in 2015]

- Yes: 71%
- No: 29%

High-profile data breaches in the news has, to some extent, driven organisation to adjust security strategy [1005 respondents in 2014]

- Yes: 53%
- No: 47%
Conclusion

The report finds that despite the fact that data breaches are on the rise and huge volumes of records are being lost or stolen worldwide, organizations continue to consider perimeter security technologies to be effective for data protection, and continue to invest more of their IT budgets in perimeter security and breach prevention technologies rather than defense-in-depth strategies that include strong multi-factor authentication and data encryption.

92%

The research found that a huge majority, 92% of IT decision-makers, said their organizations’ investments in perimeter security has either increased or stayed the same over the past five years, with an average of 9% of IT budget currently spent on purchasing, deploying and maintaining perimeter security technology.

For the next 12 months, respondents planned to continue this trend, spending about the same amount 9% on perimeter security technology.

68%

About two-thirds of the respondents (68%) also said they would not decrease spending on perimeter defenses, such as firewall technology, in favor of other technologies. If asked to get rid of one method to protect sensitive data, many would choose to eliminate anomaly detection or data security measures such as encryption rather than perimeter security.

87%

And while a significant majority of the executives surveyed (87%) think perimeter security is effective at keeping out security threats, 33% think unauthorized users are able to access their networks, and more than half (57%) admit that their organization’s perimeter security has been breached or that they do not know if it has been breached.

66%

In addition, two thirds (66%) of the respondents are not confident that their organization’s data would be secure if unauthorized users were able to penetrate their network’s perimeter security, and 15% admit that if they were a customer of their organization, they would not trust the company to store and manage their personal data.

All of this point to a lot of disconnect between how companies are spending their security budgets and their ability to protect data resources. Security and IT executives need to rethink their priorities and focus more on protecting the data than solely trying to prevent intrusions through a strong perimeter defense.

Perhaps the constant news about data breaches is having an impact and will help change attitudes about security.

71%

The survey showed that nearly three quarters of the executives surveyed (71%) said high-profile data breaches in the news have driven their organization to change its security strategy. Nearly a quarter (24%) do not feel that their organization has the security capabilities to keep up with emerging threats and technologies.