MOBILUNITY

Ukrainian Development
Western Management
Global Delivery

Outsourcing & remote teams:
cyber security vulnerabilities

Mobilunity: Cyber security research 2017-2018

In 2017 alone, 978 million people from 20 countries together lost $172 billion to cybercrimes. That's equal to the 2019 annual state government budget of New York and 17 times the 2018 annual budget of the state of Alaska. In this digital age, cyber security is unquestionably crucial. Unfortunately, only a few companies take it into consideration. Worse, businesses have common misconceptions about cyber security that impede their opportunities for growth, such as wrongly attributing cyber attacks to hiring remote developers. Here are some facts about outsourcing and cyber security, as well as some tips on how to utilize outsourcing to strengthen your IT security instead of compromising it.

Cyber Security Trends

Here are some recent cyber security trends taken from the LinkedIn Information Security Community's 2017 Cybersecurity Trends Spotlight Report.

It takes time to recover from cybercrimes.

Detecting a cyber attack takes long enough, so it is critical for an organization to recover from an attack as soon as possible. Unfortunately, this isn't always the case. Here's how long companies take to recover from attacks.

MOBILUNITY | Ukrainian Development / Western Management / Global Delivery

QUESTIONS WHICH WERE ASKED DIFFERENT COMPANIES ON THEIR CYBERSECURITY

How long did it take your organization to recover from a cyberattack?

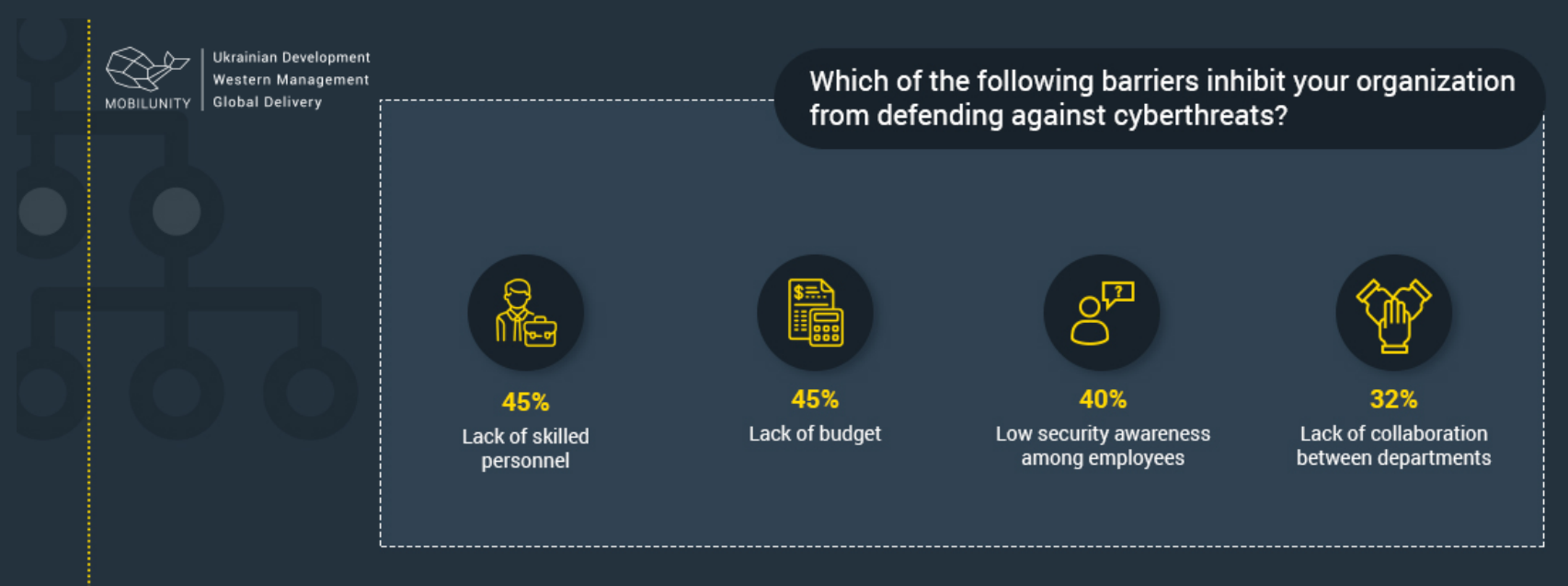| 13%	31%	25%	20%	7%	3%
Within minutes	Within hours	Within one day	Within one week	Within one month	Within three months

Cyber attacks seriously impact business operations.

Cyber attacks always negatively affect business operations. Here are some of the most common impacts of cybercrimes on organizations.
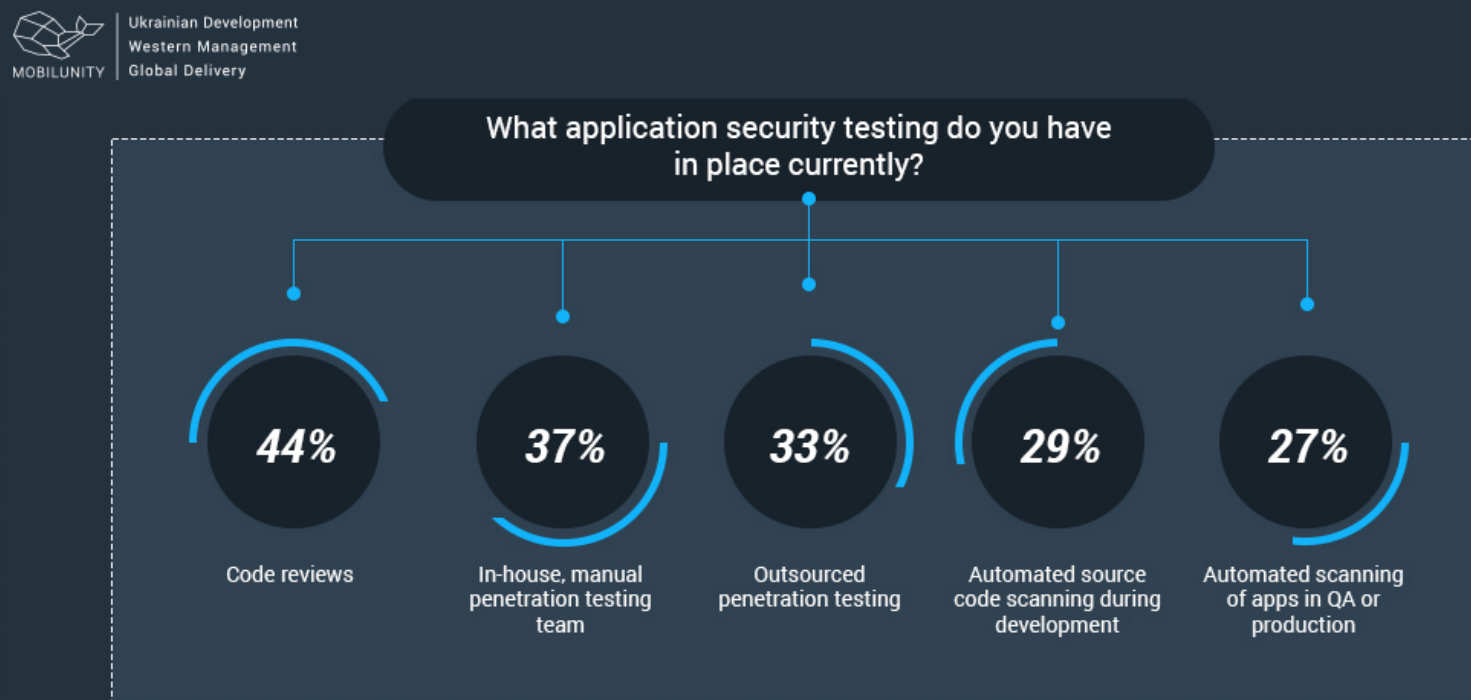

What negative impact have security incidents had on your company in the past 12 months?

MOBILUNITY | Ukrainian Development Western Management Global Delivery

41%
Disrupted business activities

33%
Reduced employee productivity

29%
Deployment of IT resources to triage and remediate issue

Lack of skills hinders companies from achieving stronger cyber security.

Several obstacles hold back organizations from strengthening their IT security, but the most common ones point to lack of IT security skills. Here are the most common hurdles that companies face.
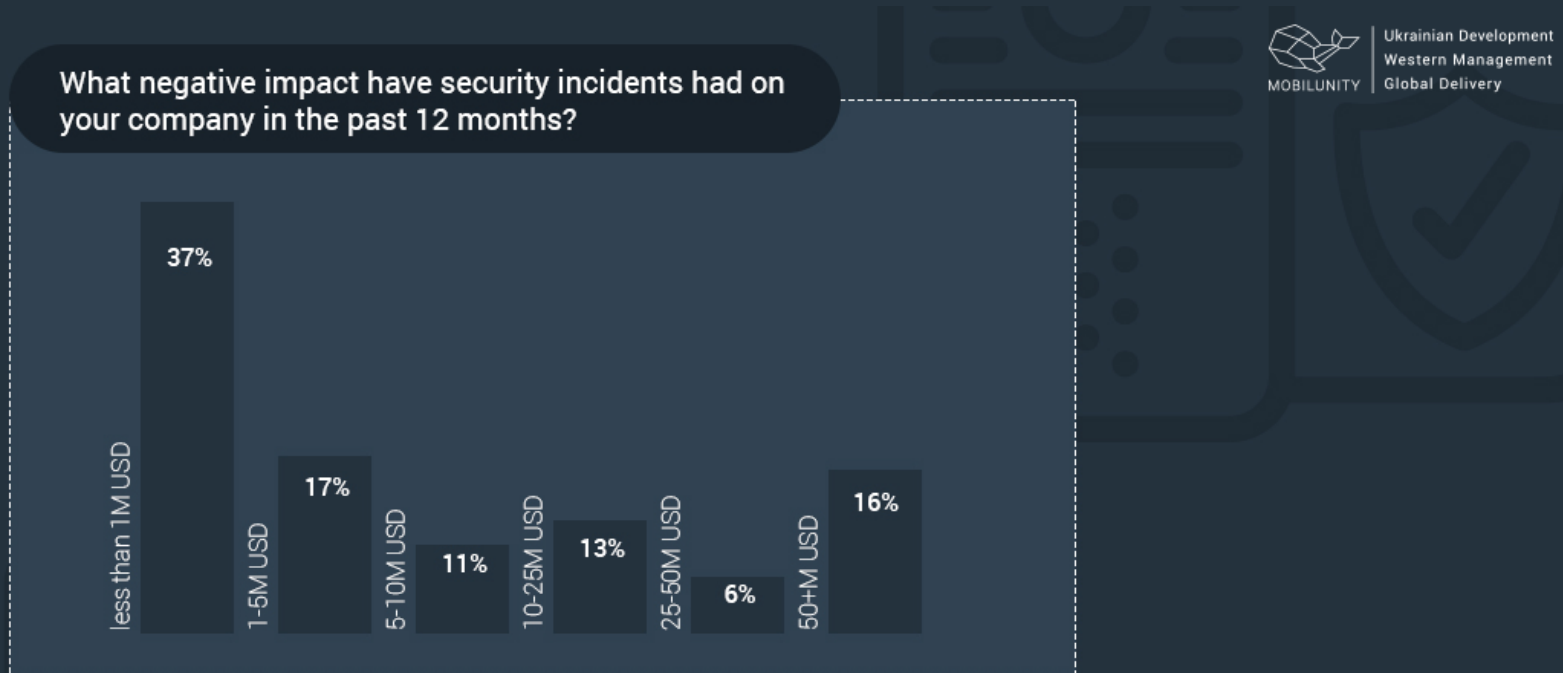

MOBILUNITY | Ukrainian Development Western Management Global Delivery

Which of the following barriers inhibit your organization from defending against cyberthreats?

45%
Lack of skilled personnel

45%
Lack of budget

40%
Low security awareness among employees

32%
Lack of collaboration between departments

sales@mobilunity.com
www.mobilunity.com

Cyber security should be a top consideration in application development.

Cyber security shouldn't be added to products as an afterthought; instead, it should be baked into the application development processes. Here are some ways by which app development companies achieve this.

Ukrainian Development
Western Management
MOBILUNITY | Global Delivery

What application security testing do you have in place currently?

44%	37%	33%	29%	27%
Code reviews	In-house, manual penetration testing team	Outsourced penetration testing	Automated source code scanning during development	Automated scanning of apps in QA or production

A SAP attack can cost a company millions.

With SAP being a highly popular enterprise resource planning (ERP) system, it's also a common target for IT security breaches. Here's how much a SAP breach actually costs companies.

What negative impact have security incidents had on your company in the past 12 months?

Ukrainian Development
Western Management
MOBILUNITY | Global Delivery

- less than 1M USD: 37%
- 1-5M USD: 17%
- 5-10M USD: 11%
- 10-25M USD: 13%
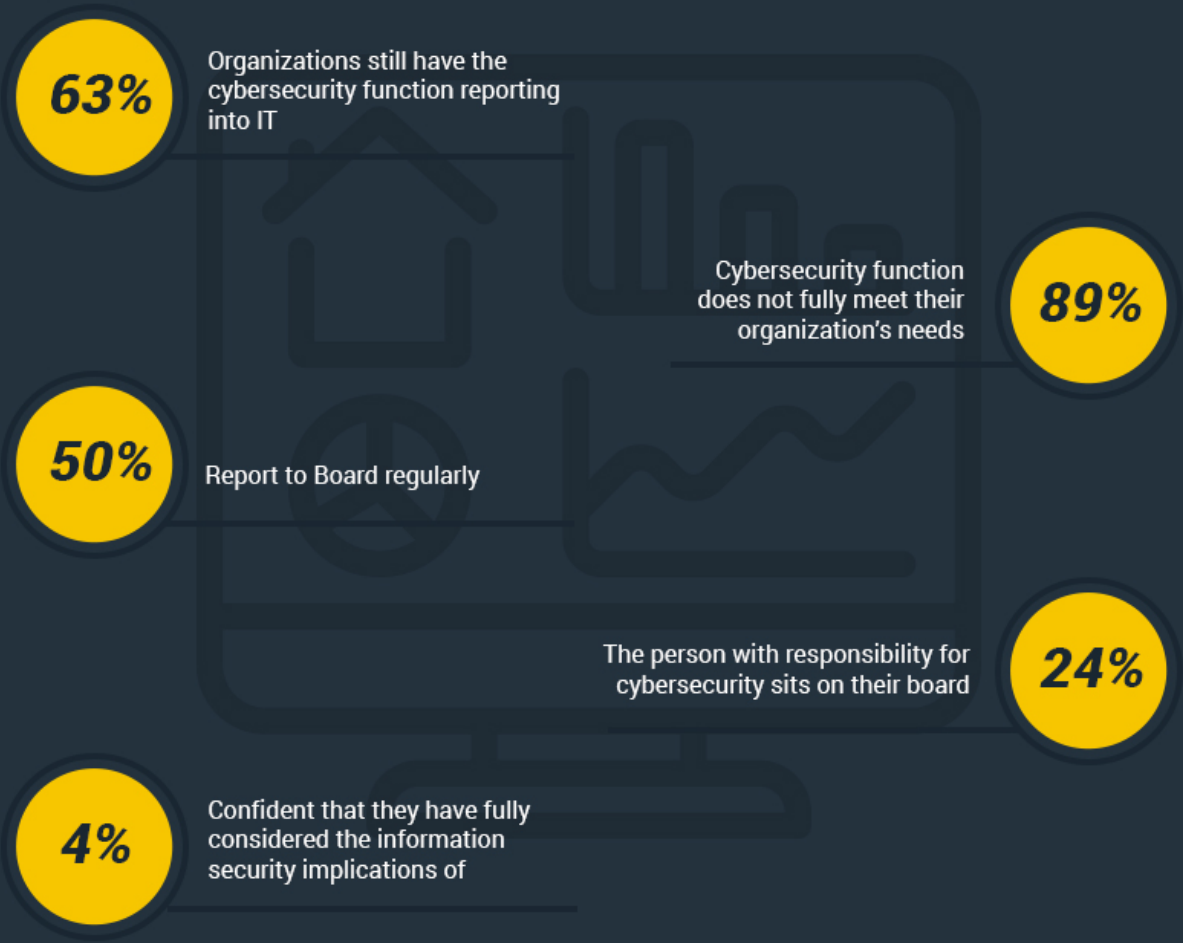- 25-50M USD: 6%
- 50+M USD: 16%

Companies need to place greater importance in their cyber security function.

The cyber security function needs to have a stronger influence within an organization. Here's how much influence cyber security functions actually have within businesses. old back organizations from strengthening their IT security, but the most common ones point to lack of IT security skills. Here are the most common hurdles that companies face.

Ukrainian Development
Western Management
MOBILUNITY | Global Delivery

COMPANIES WHICH TOOK ALL SECURITY MEASURES

63% Organizations still have the cybersecurity function reporting into IT

Cybersecurity function does not fully meet their organization's needs **89%**

50% Report to Board regularly

The person with responsibility for cybersecurity sits on their board **24%**

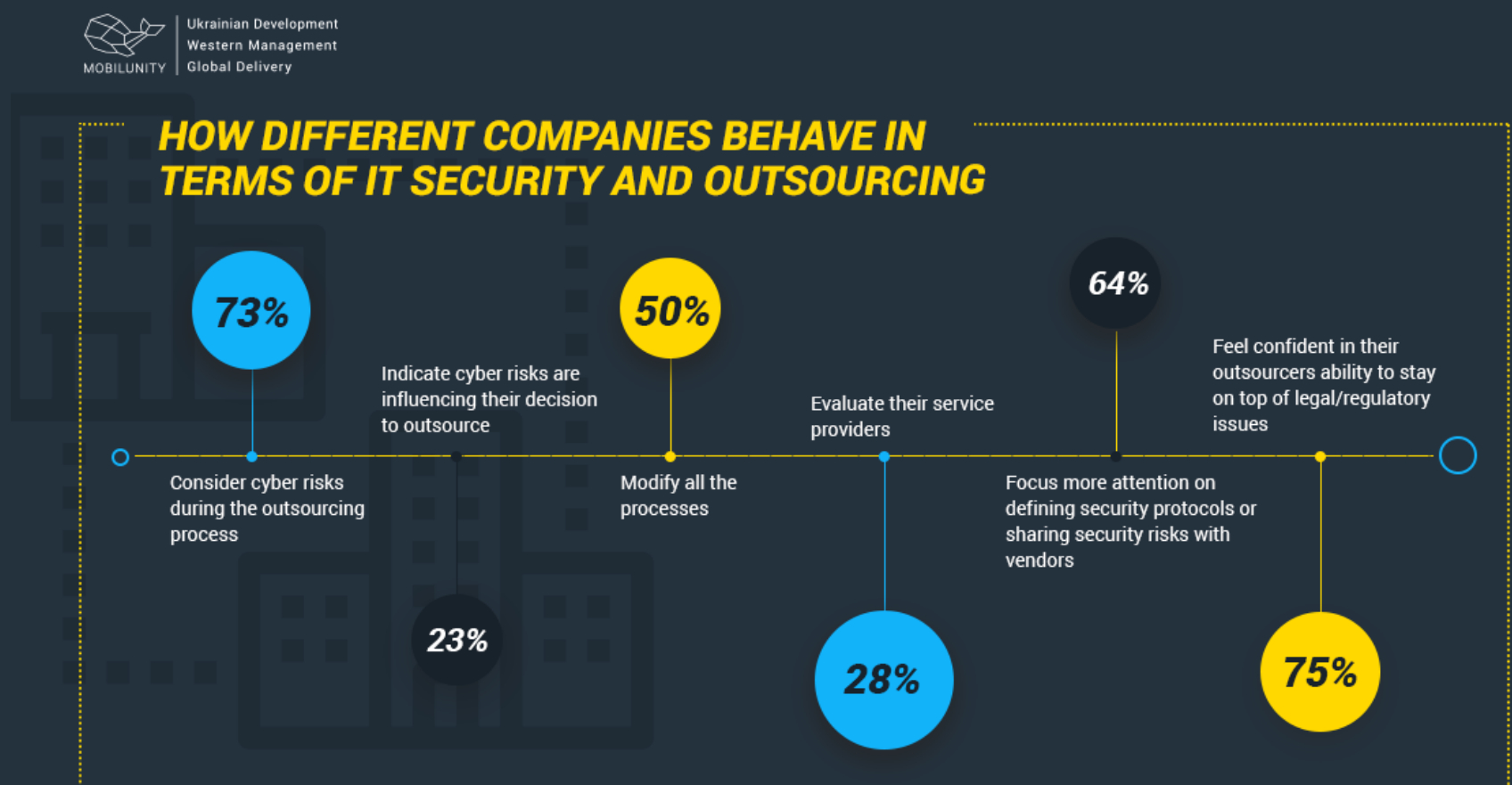**4%** Confident that they have fully considered the information security implications of

Outsourcing Trends

Many organizations have an unfounded fear that outsourcing leaves them vulnerable to cyber security threats. There is, however, very little truth to this. In fact, adherence to a proper outsourcing process is the key to a solid wall of cyber security.

Companies need to consider cyber security when outsourcing.

Cyber security should be among the first points for deliberation when outsourcing. Here's how organizations actually take cyber security into consideration when outsourcing.

MOBILUNITY | Ukrainian Development
Western Management
Global Delivery

HOW DIFFERENT COMPANIES BEHAVE IN TERMS OF IT SECURITY AND OUTSOURCING

73%

Indicate cyber risks are influencing their decision to outsource

50%

64%

Feel confident in their outsourcers ability to stay on top of legal/regulatory issues

Consider cyber risks during the outsourcing process

Evaluate their service providers

Modify all the processes

Focus more attention on defining security protocols or sharing security risks with vendors

23%

28%

75%

Global Spending on IT Security

According to Gartner, global spending on IT security was set to exceed $90 million in 2017, and this is projected to grow to $113 million in 2020.

Investing in cyber security is the way to go.
No matter how you look at it, investing in cyber security will save you a lot of time and resources in the long run. Here are some of the most common ways by which companies plan to invest in cyber security.

MOBILUNITY | Ukrainian Development
Western Management
Global Delivery

HOW DO YOU PLAN TO HANDLE YOUR EVOLVING SECURITY NEEDS IN THE NEXT 12 MONTHS?

54%

Deploy additional third-party security solutions

41%

Hire additional security professionals

Train and/or certify existing IT staff to become security experts

Partner with a managed services provider

47%

32%

Companies feel the need to increase their cybersecurity budget.
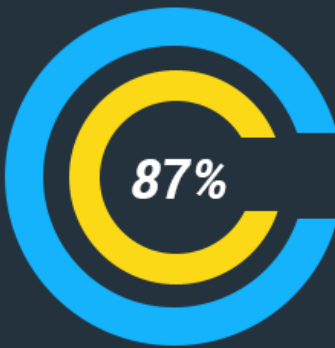
Some companies have experienced an increase in IT security budget, but many still feel the necessity for a higher cyber security budget.

HOW IS SECURITY BUDGET OF COMPANIES CHANGING IN THE NEXT 12 MONTHS

59%

Respondents this year say their budgetsincreased over the last 12 months their current strategy
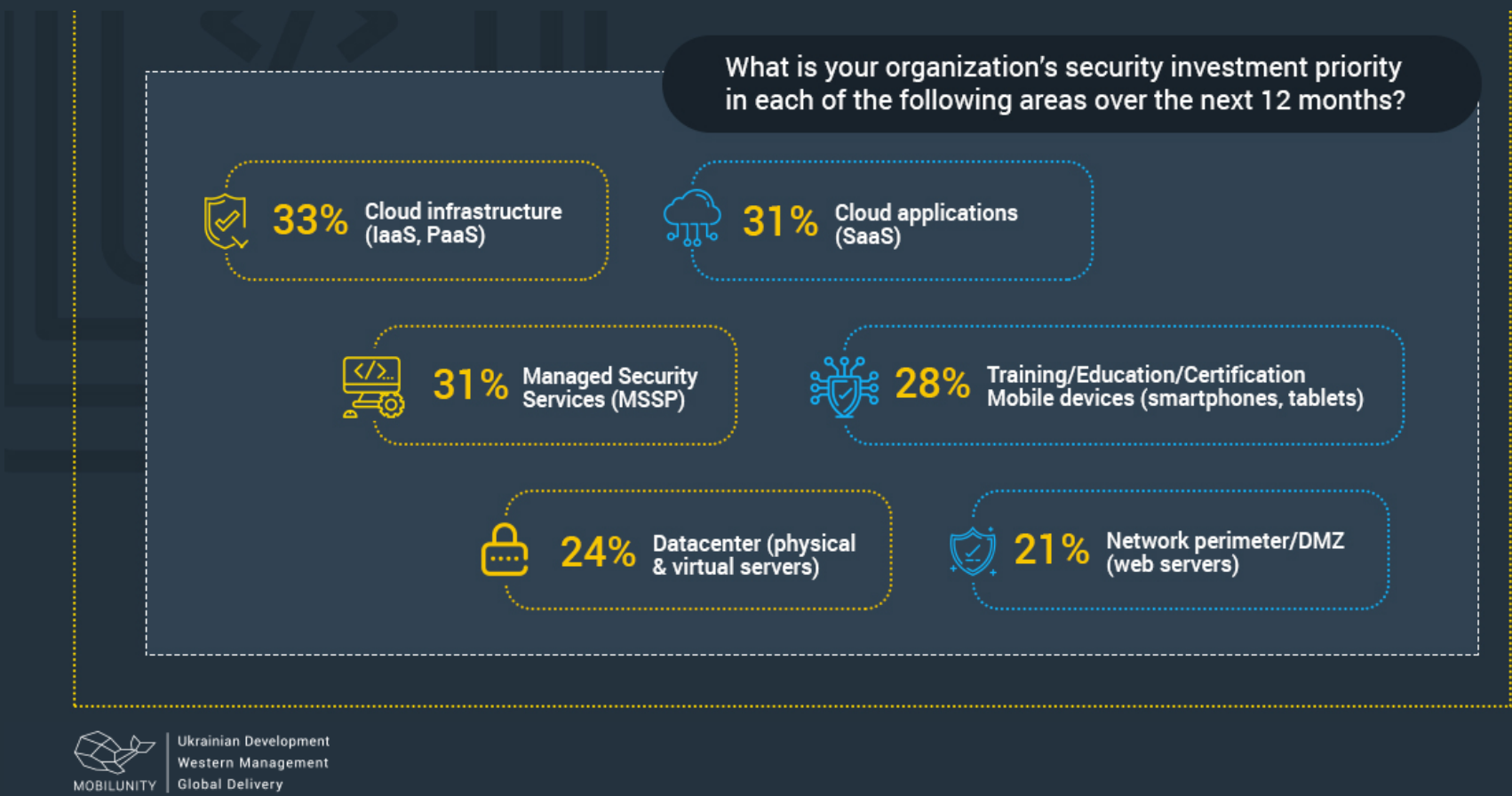
87%

Say they need up to 50% more budget

12%

Expect an increase of more than 25% in their cybersecurity budget

Many companies plan to invest in cloud cybersecurity.

Organizations have varying priorities in terms of how to invest in cyber security, but among the top methods is to invest in cloud infrastructure. Here are the most common ways companies plan to invest in cyber security.

What is your organization's security investment priority in each of the following areas over the next 12 months?

33% Cloud infrastructure (IaaS, PaaS)

31% Cloud applications (SaaS)

31% Managed Security Services (MSSP)

28% Training/Education/Certification Mobile devices (smartphones, tablets)

24% Datacenter (physical & virtual servers)

21% Network perimeter/DMZ (web servers)

MOBILUNITY | Ukrainian Development
Western Management
Global Delivery

sales@mobilunity.com
www.mobilunity.com

How to Strengthen Cyber Security when Outsourcing

While organizations incorrectly attribute cloud security breaches to outsourcing, hiring remote developers can actually lead to strengthened IT security when done properly. Here are some things to consider when outsourcing in order to boost your cyber security.

Hire only from ISO-Certified companies.

Adherence to ISO standards ensures that your outsourcing partner follows the strictest standards in business operations set forth by the International Organization for Standardization. For information security, ISO/IEC 27001 certification should be on top of your checklist.

Implement early security evaluation.

Early Security Evaluation is when cyber security is considered in the first stages of software development. This ensures that security is thoroughly given due consideration during the entire development process.

Make sure your outsourcing partner complies with data regulations.

Ensuring that your partner company follows data protection laws, such as the General Data Protection Regulation (GDPR) in European regions, ensures that your sensitive information is properly handled and secured.

References:
https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
https://www2.deloitte.com/us/en/pages/operations/articles/key-insights-from-deloitte-2016-outsourcing-survey.html
https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-re-gained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf
https://www.gartner.com/newsroom/id/3638017
https://www2.deloitte.com/us/en/pages/operations/articles/key-insights-from-deloitte-2016-outsourcing-survey.html

sales@mobilunity.com
www.mobilunity.com