ВЛИЯНИЕ МОБИЛЬНЫХ УСТРОЙСТВ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ:

ОПРОС IT-ПРОФЕССИОНАЛОВ

Июнь 2013

dimensional research

При поддержке Check Point SOFTWARE TECHNOLOGIES LTD.

ВЛИЯНИЕ МОБИЛЬНЫХ УСТРОЙСТВ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ:
ОПРОС IT-ПРОФЕССИОНАЛОВ

Dimensional Research | Июнь 2013

Вступление

Мобильные устройства вызывают постоянное беспокойство у IT-команд, ответственных за информационную безопасность. Конфиденциальная корпоративная информация может быть легко вынесена и потеряна, при этом феномен Bring Your Own Device (BYOD, Принеси Своё Устройство) резко увеличил количество дорогостоящих инцидентов безопасности.

Данный доклад, выполненный при поддержке Check Point, основан на глобальном опросе 790 IT-профессионалов, проведённом в США, Канаде, Великобритании, Германии и Японии. Это второй опрос на эту тему, и в докладе проведено сравнение с ответами на те же вопросы, заданные год назад. Целью опроса был сбор данных для количественной оценки влияния мобильных устройств на корпоративную информационную безопасность.

Резюме

1. BYOD быстро растёт и затрагивает предприятия любых масштабов
2. Корпоративная информация на мобильном устройстве – более ценное имущество, чем само мобильное устройство
3. Инциденты мобильной безопасности обходятся дорого, даже малому и среднему бизнесу.

Основные выводы

- **К корпоративным сетям подключается всё больше мобильных устройств**
  - 93% имеют мобильные устройства, которые подключаются к их корпоративной сети
  - 67% позволяют подключаться к корпоративным сетям личными устройствами
- **BYOD быстро растёт и создаёт проблемы для организаций**

  Среди компаний, которые позволяют подключаться к корпоративным сетям личными устройствами:
  - 96% отмечают рост количества таких устройств
  - 45% получили более чем пятикратный прирост количества личных устройств за последние два года (в прошлом году эта доля составляла 36%)
  - 63% не управляют корпоративной информацией на личных устройствах
  - 93% сталкиваются с проблемами, внедряя политики касательно BYOD
  - Защита корпоративной безопасности упоминается как главная проблема BYOD (67%)
- **Данные клиентов на мобильных устройствах вызывают опасения нарушения безопасности**
  - 53% сообщают о наличии конфиденциальных данных клиентов компании на мобильных устройствах, что выше, чем 47% год назад
  - 94% выражают серьёзную озабоченность случаями утери или кражи данных клиентов как проблемой мобильной безопасности
- **Инциденты мобильной безопасности очень дорого обходятся**
  - 79% сообщают об инцидентах мобильной безопасности в прошедшем году
  - 52% крупных компаний говорят, что потери от инцидентов мобильной безопасности за прошлый год превысили $500000
  - 45% компаний с менее 1000 работников сообщают об инцидентах мобильной безопасности, которые обошлись в более, чем $100000
  - 49% упоминают Android как платформу с наибольшим предполагаемым риском безопасности (что выше, чем 30% в прошлом году), по сравнению с Apple, Windows Mobile и Blackberry
  - 66% говорят, что беспечные работники – это больший риск безопасности, чем киберпреступники

dimensional research

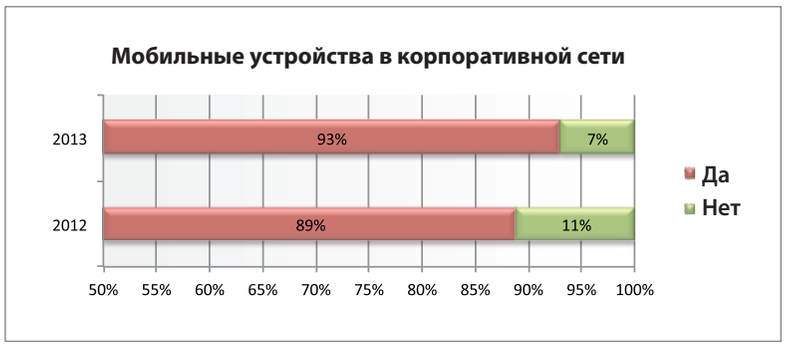
При поддержке Check Point SOFTWARE TECHNOLOGIES LTD.

www.dimensionalresearch.com

Подробные выводы

Широкое использование мобильных устройств в корпоративных сетях

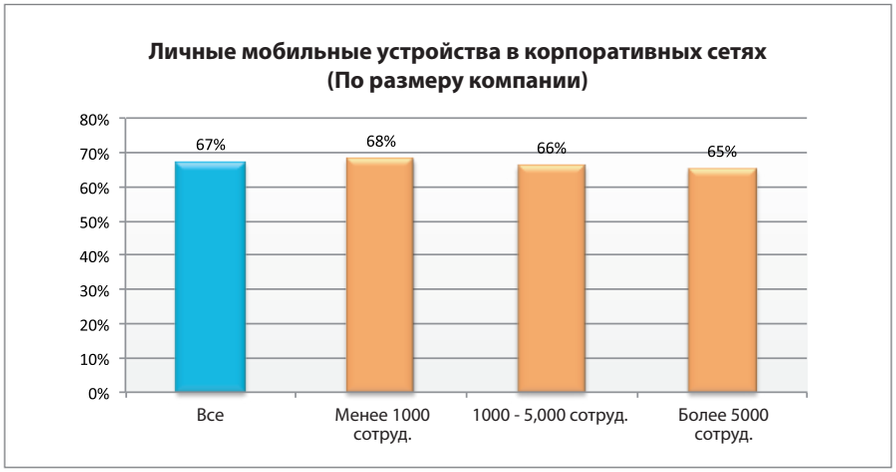
Участников спрашивали, подключены ли мобильные устройства, такие как смартфоны и планшеты, к их корпоративной сети. Было отмечено широкое использование мобильных устройств, а именно 93% сообщили, что имеют мобильные устройства, подключающиеся к их корпоративной сети. Это больше, чем 89% в 2012.



Больше корпоративных сетей содержат личные устройства

Чуть больше двух третей организаций, 67%, позволяют устройствам в личном владении работников, наёмных сотрудников или других людей, подключаться к их корпоративным сетям. В это число входят 65% тех, у кого в сети и личные, и корпоративные устройства и 2% тех, у которых мобильные устройства исключительно личного владения. Это больше, чем 65% в 2012.

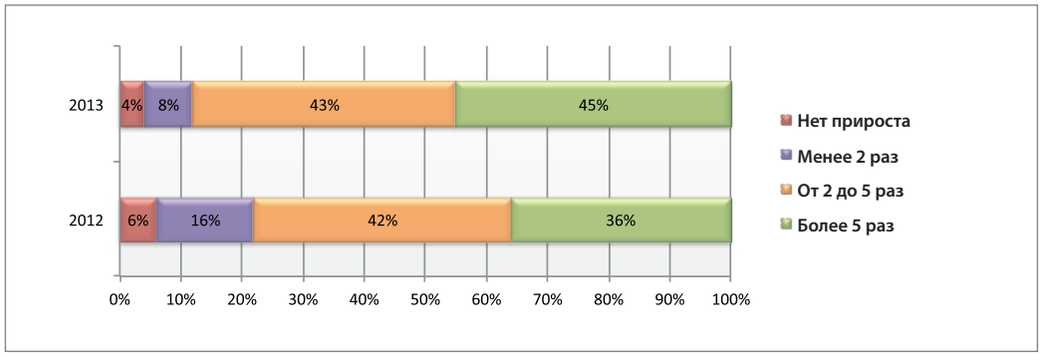
Использование личных мобильных устройств одинаково в компаниях любого размера. Количество предприятий, имеющих личные устройства в корпоративных сетях, слабо варьируется от наименьших (68%) до наикрупнейших (65%).



Личные мобильные устройства продолжают распространение.

У тех IT-профессионалов, чьи компании разрешают мобильным устройствам в личном владении подключаться к корпоративной сети, мы спросили, каков был прирост за последние два года. Подавляющее большинство, 96%, отметили рост в использовании мобильных устройств в корпоративной сети. В некоторых компаниях рост был очень резким, так что 45% сообщили, что у них в сети мобильных устройств более чем в пять раз больше, чем два года назад.

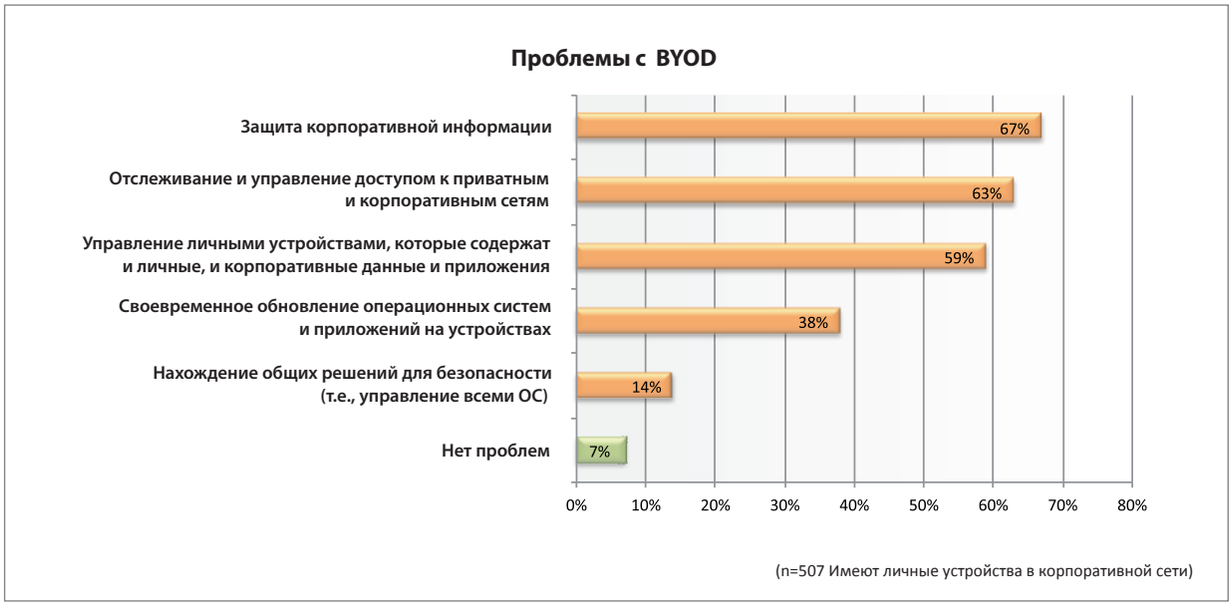
Этот рост в этом году ещё более резок, чем в прошлом. В 2012 мы задавали тот же вопрос. Только 36% компаний имело рост более, чем в пять раз, по сравнению с 45% в опросе этого года



Защита корпоративной информации как главная задача в адаптации BYOD

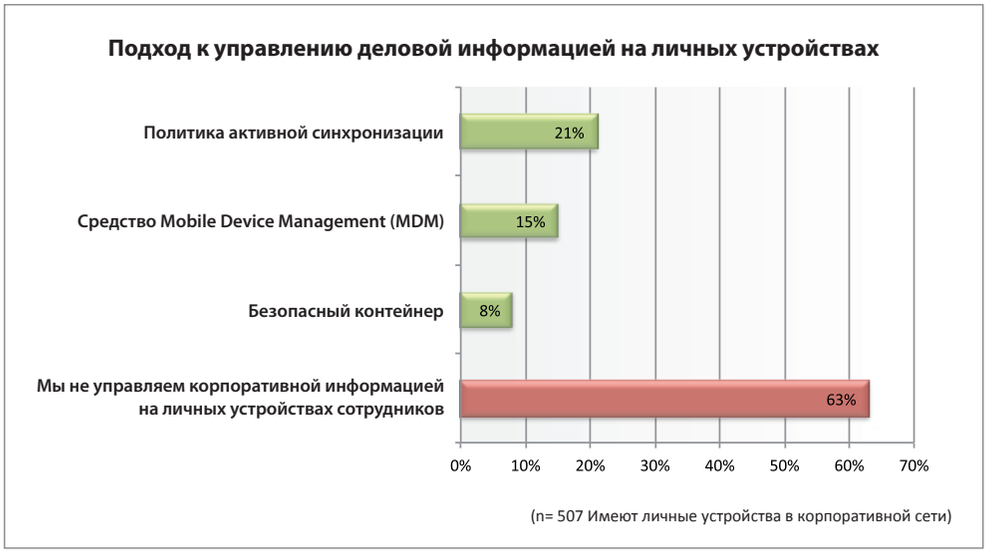
BYOD вызывает проблемы у корпоративных IT. Подавляющее большинство компаний, разрешающих личные устройства в своих сетях, 93%, сообщили, что когда работники используют свои смартфоны, планшеты или другие устройства для работы с деловой информацией, это приводит к проблемам.

Участники сообщили, что самой частой проблемой при адаптации BYOD была защита корпоративной информации (67%), следом за которой идёт отслеживание и контроль доступа к сетям (63%).

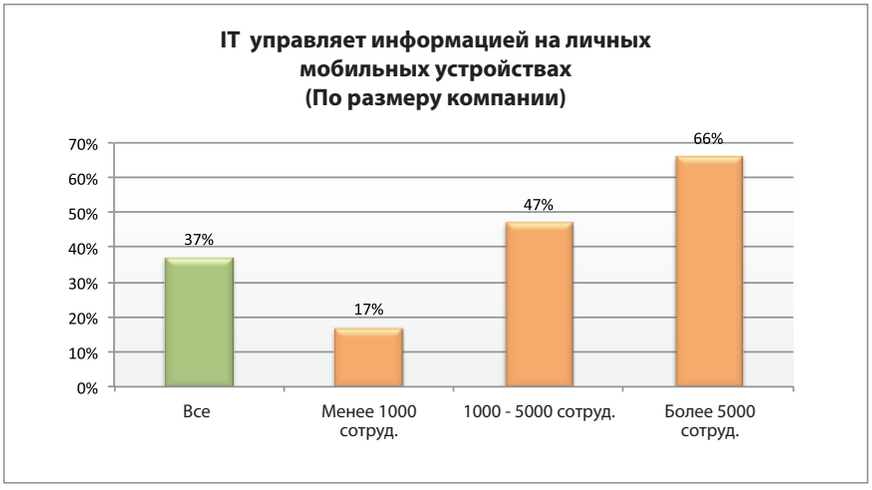


Корпоративная информация на личных устройствах, не контролируемая IT

Почти две трети, 63%, компаний, разрешающих мобильным устройствам в частном пользовании подключаться к своим корпоративным сетям, не контролируют корпоративную информацию, находящуюся на них. Среди тех, кто контролирует, наиболее распространены политики активной синхронизации (21%), после них средства Mobile Device Management (MDM) (15%), и безопасный контейнер (8%).



Для крупных компаний более характерно управление корпоративной информацией на личных устройствах. Очень малая доля компаний с менее 1000 сотрудников, 17%, использует технический подход к управлению информацией на мобильном устройстве сотрудника, это гораздо меньше, чем 66% от компаний с более 5000 сотрудников.



В наши дни на мобильных устройствах всё больше типов информации

Участники отметили прирост по всем видам информации, хранимой на мобильных устройствах, по сравнению с прошлым годом. Корпоративная почта, самый распространённый в ответах вид корпоративных данных, выросла с 79% мобильных устройств в прошлом году до 88% в этом.

Больше стало компаний, конфиденциальные данные которых попадают на мобильные устройства. Хранение данных клиента на мобильных устройствах выросло с 47% в 2012 до 53% в 2013. Наибольший прирост показала доля корпоративной информации, попадающей на мобильные устройства через бизнес-приложения, прибавив 17% с 2012 по 2013.

Возможность утери корпоративной информации через мобильные устройства вызывает наибольшую озабоченность

Инциденты мобильной безопасности могут иметь весьма разнообразные последствия. Участникам опроса предложили список возможных последствий и предложили расположить их по убыванию от наиболее к наименее значимым. Потерянные или украденные устройства были отмечены номером 1 как фактор, имеющий наибольшее влияние на уязвимость мобильных данных; следующими были отмечены вредоносные программы, установленные на мобильное устройство. Большая доля пользователей, меняющих или обновляющих свои мобильные устройства, была отмечена как наименее значимый фактор.

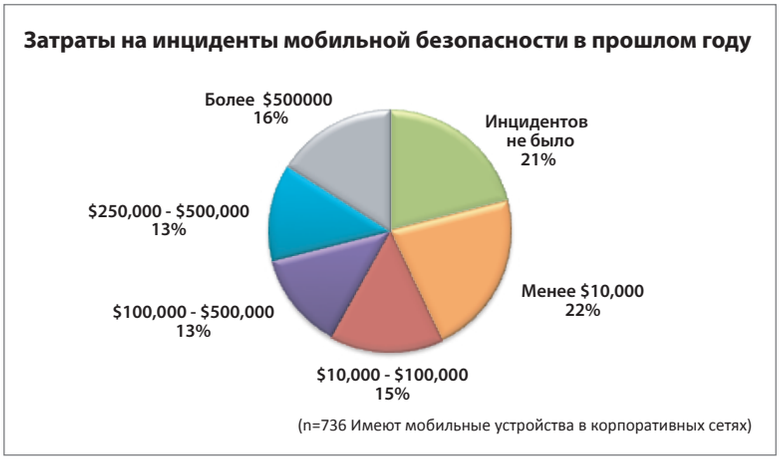
При инциденте мобильной безопасности опаснее всего – утеря корпоративной информации

Инциденты мобильной безопасности могут иметь весьма разнообразные последствия. Участникам, имеющим как личные, так и корпоративные мобильные устройства в своих сетях, было предложено выбрать самые тревожащие из списка возможных проблем, которые могут возникнуть как результат инцидента мобильной безопасности.

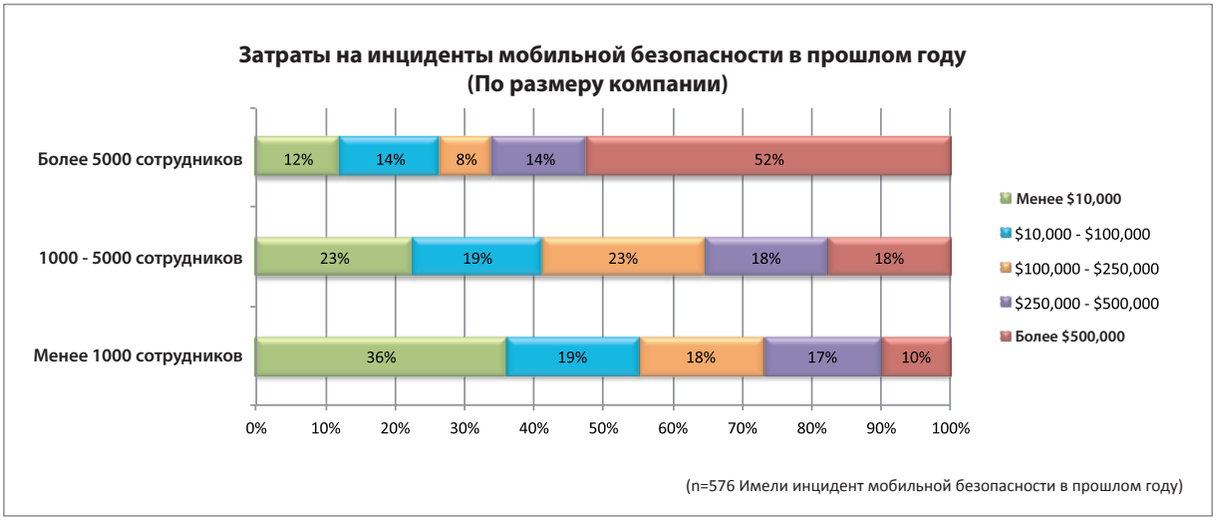
Возможность потери корпоративной информации оказалась на первом месте с большим отрывом (94%). Затраты на замену украденного устройства оказались на втором месте (20%).

Инциденты мобильной безопасности обходятся дорого

Как только в компании появляются мобильные устройства, происходят инциденты безопасности и ущерб от них существенен. Большинство компаний из имеющих в своих сетях мобильные устройства, 79%, имели хотя бы один инцидент мобильной безопасности в прошлом году. Большинство, 57%, сообщили, что общие затраты на эти инциденты мобильной безопасности составили от $10000 до свыше $500,000 в прошлом году. В эти затраты входят время персонала, судебные издержки, штрафы, процессы урегулирования и так далее.



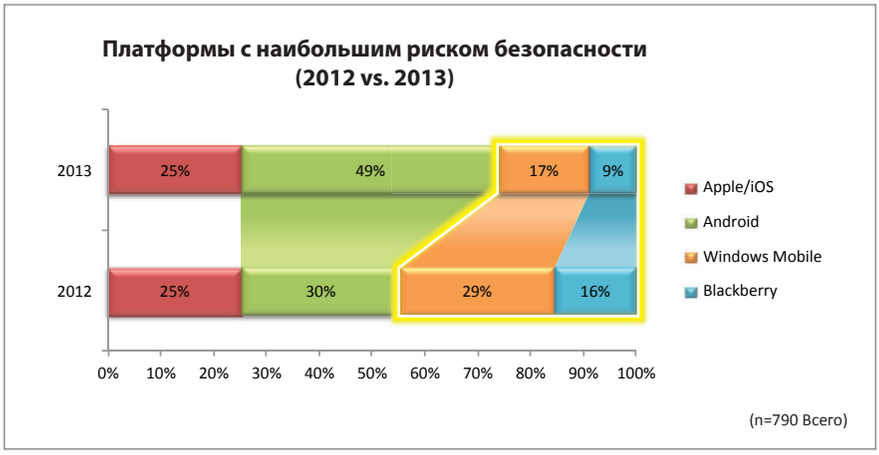
Когда происходили инциденты безопасности, наиболее существенными были затраты в крупнейших компаниях. Из тех, кто работает в компаниях с более 5000 сотрудников, больше половины (52%) сообщили, что за прошлый год затраты на инциденты мобильной безопасности превысили $500000. Впрочем, даже малые и средние предприятия сообщали, что инциденты мобильной безопасности были очень дорогостоящими. Почти половина компаний с менее 1000 сотрудников, 45%, сообщили об инцидентах безопасности, стоивших более $100000, значительная сумма для маленькой фирмы.



Android'у меньше, а Windows Mobile и BlackBerry больше доверяют в безопасности

Участников спросили, какие из наиболее распространённых мобильных платформ, которые они рассматривали, являются наибольшим риском для их корпоративной безопасности. Android был назван первым с большим отрывом (49%), за ним следует Apple/iOS (25%) и Windows Mobile (17%).

По этому вопросу наблюдается резкая перемена по сравнению с прошлым годом. Android сильно прибавил в качестве платформы с наибольшим предполагаемым риском. И Windows Mobile, и BlackBerry потеряли почти половину IT-профессионалов, рассматривавших их как максимально рискованную платформу.



Беспечные сотрудники считаются большим риском для безопасности, чем киберпреступники

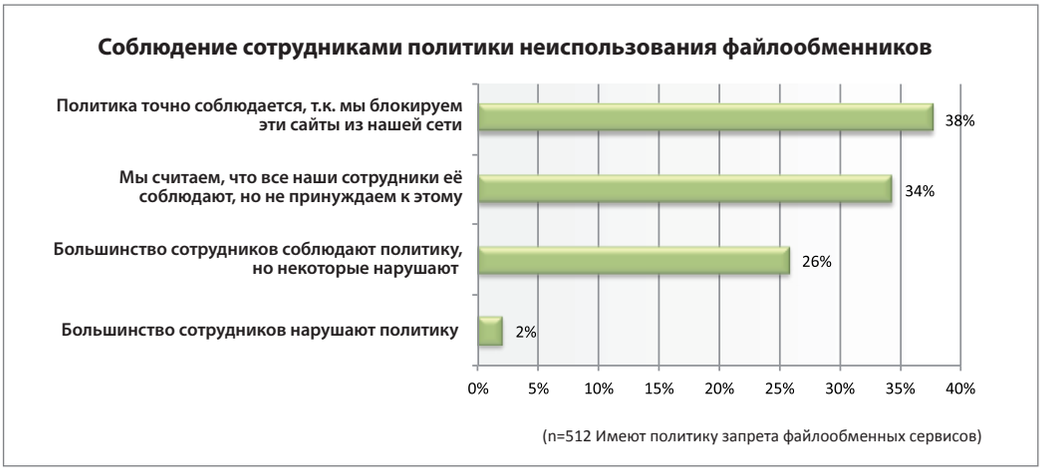
Участников спросили, какая группа лиц предполагается наибольшим риском для безопасности — беспечные сотрудники или киберпреступники, которые умышленно пытаются украсть корпоративную информацию. Гораздо больше ответили, что беспечные сотрудники представляют собой больший риск (66%), нежели киберпреступники (34%). Этот факт подкрепляет важность реализации сильного сочетания технологий с осведомлённостью о безопасности во всей организации.

IT может не позволять использовать файлообменники, но эта политика часто не форсируется

Использование мобильных устройств привело к повсеместному пользованию файлообменниками, такими как DropBox, Box, Google Drive и iCloud, которые некоторые IT-организации воспринимают как угрозу для безопасности корпоративных данных. Участников спросили, можно ли их сотрудникам закачивать и обмениваться рабочей информацией посредством публичных файлообменных приложений. Организации разделились на те, чьи политики разрешают делать это всем сотрудникам (35%) и те, чьи не разрешают никому из сотрудников (25%). Большинство же разрешает части сотрудников и запрещает остальным (40%).

При этом эти ограничения применяются не одинаковым образом. В организациях, которые имеют политику ограничений для некоторых своих сотрудников в использовании публичных файлообменников, мы спросили, считают ли они, что эта политика соблюдается.

Только 38% действительно реализуют свою политику путём блокировки этих сайтов в корпративных сетях, в то время как 28% признают, что некоторые сотрудники эту политику не соблюдают.



Методология опроса

Для участия в онлайн-опросе на тему мобильных устройств и информационной безопасности при поддержке Check Point была привлечена независимая база IT-профессионалов. В общей сложности 790 респондентов из США, Канады, Великобритании и Японии приняли участие в опросе. Каждый респондент отвечает за безопасность систем своей компании. Участники являются ИТ-руководителями, ИТ-менеджерами и прикладными ИТ-специалистами, и представляют широкий спектр размеров компаний и производственных вертикалей.

Этот опрос – второй в серии опросов на эту тему. Этот доклад сравнивает выборочные ответы на похожие вопросы, заданные год назад.

О Dimensional Research

Dimensional Research® проводит практические маркетинговые исследования, чтобы помочь технологичным компаниям делать своих клиентов более успешными. Наши исследователи – эксперты в вопросах людей, процессов и технологий корпоративных IT структур и они понимают, как работают IT организации. Мы сотрудничаем с нашими клиентами, чтобы получить полезную информацию, которая снижает риски, повышает удовлетворённость клиентов и позволяет бизнесу расти.
Дополнительная информация – на сайте www.dimensionalresearch.com.

О Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), мировой лидер в вопросах безопасности Интернета, обеспечивает клиентам бескомпромиссную защиту от всех типов угроз, снижает сложность реализации систем безопасности и снижает общую стоимость владения. Check Point были первыми в этой отрасли с FireWall-1 и патентованной технологией контроля состояния соединений. Сегодня Check Point продолжает развивать инновации на основе Software Blade.

Архитектура, предоставляющая клиентам гибкие и простые решения, полностью настраиваемые для лучшего соответствия требования безопасности любой компании. Check Point является единственным поставщиком, вышедшим за рамки технологий и определившим безопасность как бизнес-процесс. Check Point 3D Security уникально сочетает в себе политику, людей и фокусировку на лучшей защите информационных активов и помогает организациям реализовать план безопасности, который совпадет с потребностями бизнеса.

Клиентами компании являются десятки тысяч организаций всех размеров, в том числе все компании Fortune и Global 100. ZoneAlarm, титулованный продукт Check Point, защищает миллионы пользователей от хакеров, шпионских программ и кражи конфиденциальной информации.