Вопросы кибербезопасности при удаленной работе в условиях COVID-19.

Илья Кравцов
Руководитель IBM Security в России и СНГ

IBM **Security**

IBM

Реакция на COVID-19 — Приоритеты ИБ при удаленной работе

Обеспечить непрерывность ИБ

- Поддерживать работу службы ИБ в режиме 24/7
- Перейти на удаленное реагирование на инциденты

Быть готовым к новым угрозам

- Бдительность и осведомленность
- Обеспечить безопасность удаленной работы
- Понимать возросшие риски

Обеспечить готовность IT

- Определить критичные функции и сотрудников
- Обеспечить сотрудников необходимыми ресурсами
- Проработать план отказоустойчивости

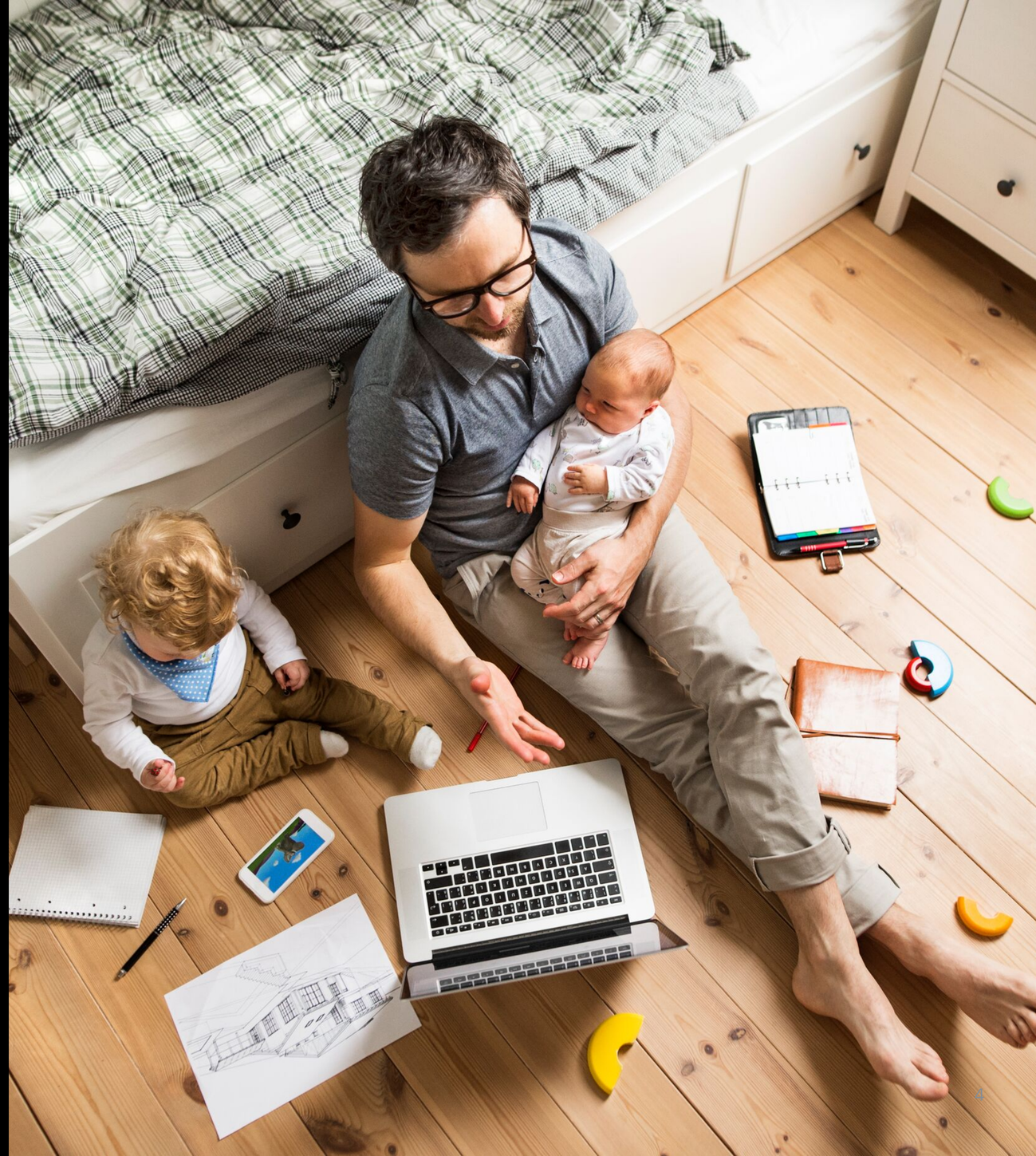
Ограничения и риски удаленной работы

- У многих сотрудников нет защищенных корпоративных устройств
- Пропускная способность домашних сетей зачастую недостаточна для выполнения служебных обязанностей
- Масштабирование вычислительной инфраструктуры и поддержание ее в рабочем состоянии затруднены
- Резко возросшая нагрузка на корпоративные VPN-соединения
- Сотрудники используют домашние устройства, которые не защищены корпоративными средствами безопасности и контроля
- Неопределенность в вопросах соблюдения требований регуляторов

9

Рекомендаций для безопасной удаленной работы

1. Напомните сотрудникам о правилах безопасной работы из дома
2. Используйте корпоративные средства связи и совместной работы
3. Не используйте внешние сервисы для рабочих нужд
4. Пользуйтесь корпоративными устройствами для работы и соблюдайте политики безопасности
5. Будьте бдительны и помните о социальной инженерии
6. Соблюдайте гигиену нахождения в сети
7. Используйте двухфакторную аутентификацию
8. Обеспечьте необходимую пропускную способность VPN
9. Проводите тестирование на проникновение и безопасность приложений



Спасибо

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity