Digitalization and cybersecurity: confrontation or partnership

Good afternoon, dear friends!

Slide 1: Much has been said today about digitalization. And of course the future of human society is connected with the use of high-technology at all activity levels and today our objective is to make these technologies not only convenient but also safe.

2. The growth of mobile apps and services in use, the volume of processed data, the development of artificial intelligence technologies, and cloud services not only increases the range of available hacker attacks, but also creates damages of cyberattacks increasingly significant to operations.

The damage cost is growing rapidly. According to cybersecurity ventures, the damage cost of cyberattacks was 6 trillion dollars, that means 500 million per month... etc.

That's why it is paid more attention to the cybersecurity recently.

Slide 3: In order for information security not to be so expensive, but a full partnership that helps the company to develop we need 3 things:

1. Built-in security

Historically, most application and data protection solutions have been developed separately and they are an additional setting to the existing infrastructure. This approach provides a much lower security level as it does not allow to use built-in capabilities of the software.

Due to the growing number of complex and targeted attacks, developers and customers with increasing frequency are turning to the secure-by-design concept, which is expected to cover security requirements at the earliest stages of creating a product or service.

2. Agile

Agile methodologies in project management have become a de facto standard for technology companies, and then began to spread beyond development departments to other industry sectors, and now Agile practices applied in security as well.

Today, knowledge of Agile methods and practices is considered mandatory for both information security managers and specialists, especially when they are members of development teams.

3. Business process security (last but not least)

Perhaps the most significant quality step towards protecting companies is the shift the focus of protection from infrastructure to the core, that creates profitable business processes. It is often necessary to protect not only the infrastructure, but also the people working on it, who are also vulnerable to social engineering attacks. By the way, the weakest link of information security is not infrastructure or applications, but people.

This approach is highly common and requires a high level of organizational maturity, and a qualified information security manager who understands the business well and is part of the company's management.

Modern Business

Modern business is an ultra-technological racing car in which fuel is money, the driver is management, the engine is the production departments, indicators are accounting and controlling, and information security is the brake system.

Contrary to popular belief, the brakes not only decelerate, but also help you go the distance faster and safer and it is a key component of successful overtaking.

A holistic view of business and solidarity of purpose is the key to a successful digital transformation. Cybersecirity takes its place as a full partner by accelerating changes, protecting new values and providing a competitive edge. It is not easy and requires a transformation of

information security services, long-term investment and patience. All of these become an opportunity to stay ahead and compete for leadership.

Цифровизация и кибербезопасность – противостояние или партнерство

Добрый день, друзья!

1 слайд: Сегодня много было сказано о цифровизации и да будущее человеческого общества неотъемлемо связано с использованием высоких технологий на всех уровнях деятельности и сегодня нашей задачей является сделать эти технологии не только удобными, но и безопасными.

2. Рост количества используемых мобильных приложений и сервисов, объема обрабатываемых данных, развитие технологий искусственного интеллекта и облачных услуг не только увеличивает доступный злоумышленникам ландшафт, но и делает ущерб от кибератак все более значимым для операционной деятельности.

Стоимость ущерба стремительно растет и в абсолютных значениях. По данным cybersecurity ventures стоимость ущерба от кибератак составило 6 триллионов долларов, а это как вы видите: 500 млн в месяц… и тд

Именно поэтому в последнее время уделяется больше внимания вопросам кибербезопасности.

Слайд 3. Для того, чтобы ИБ была для бизнеса не затратным центром или регуляторным щитом, а полноценным партнером, который помогает компании развиваться и зарабатывать деньги необходимы:

1. Встроенная безопасность

Исторически большинство решений по защите и приложений и данных разрабатывались отдельно и представляют собой надстройку над существующей инфраструктурой. Подобный подход обеспечивает значительно более низкий уровень безопасности, так как не позволяет использовать встроенные возможности программного обеспечения.

Из-за растущего числа сложных и целенаправленных атак разработчики и заказчики все чаще обращаются к концепции secure by design, которая предполагает включение требований по безопасности на самых ранних этапах создания продукта или сервиса.

2. Agile

Гибкие методологии в управлении проектами стали стандартом де-факто для технологических компаний, а затем начали распространяться за пределы отделов разработки и в другие сектора промышленности, в том числе Agile-практики теперь применяются и в области безопасности.

В настоящее время знание методов и практик Agile считается обязательным, как для менеджеров по информационной безопасности, так и для специалистов, особенно в случаях, когда те являются членами команд разработки.

3. Безопасность бизнес процессов

Возможно, что самый существенный качественный скачок в подходах к защите компаний –смещение фокуса защиты от инфраструктуры к основным, формирующим прибыль бизнес-процессам. Ведь зачастую защищать нужно не только инфраструктуру, но и людей работающих на ней, которые также подвержены атакам путем социальной инженерии. К слову самым слабым звеном информационной безопасности являются не инфраструктура, не приложения, а именно люди.

Такой подход наблюдается все чаще и требует высокой организационной зрелости, и квалифицированного руководителя ИБ, который хорошо понимает бизнес и входит в руководство компании.

Современный бизнес

Современный бизнес – это сверхтехнологичный гоночный болид, в котором топливо – деньги, пилот – руководство, двигатель – производственные отделы, индикаторы и телеметрия – бухгалтерия и контролинг, а ИБ – тормозная система.

Вопреки распространенному мнению тормоза не только не замедляют, они помогают проходить дистанцию быстрее и безопаснее и, что, возможно, еще важнее, являются ключевым компонентом успешных обгонов.

Холистический взгляд на бизнес и общность целей – залог успешной цифровой трансформации, в которой ИБ занимает место полноправного партнера, ускоряя изменения, обеспечивая защиту новых ценностей и предоставляя конкурентные преимущества. Это не просто и требует преобразований в службах информационной безопасности, долгосрочных инвестиций и терпения, что с лихвой окупается возможностью быть впереди и бороться за лидерство.