SECURE CODE WARRIOR

securecodewarrior.com

# How Has 2020 Changed the Way We Look at Software Security?

## Executive Roundtable Summary

25 February 2021

### Featured Subject Matter Experts:


**Espen Agnalt Johansen**
Director of Security
Visma

**Maria Morris**
Application Security Engineer
Blue Prism

**Per Olsson**
Application Security Engineer
Visma

# Event Synopsis

Technology has had a pretty great year, but what does this mean for security? In this executive roundtable luncheon, we heard from some of our favorite subject matter experts on their feedback around the following topics:

- How have organizations changed to be more digital focused because of COVID-19, and how will this impact the future?
- As organizations start to think more strategically than reactively in their digital focus how will this impact software security?
- With more and more staff using tech, how do we focus on upskilling those who are responsible for the development and security of our software?

*In this document, we share the thoughts of the attendees of this roundtable, including opinions and experiences. Therefore, this is a summary of a discussion, and does not include references or supporting documentation.*

## How has 2020 changed the way that organizations look at Software Security?

Being a large enterprise technology company, Visma has the benefit and responsibility of having teams based all over the world. Traditionally, they would take the time to travel to those different locations and deliver hands-on security training to the developer teams, supported by e-learning. This was a great opportunity to engage with the teams and make sure that they had interactive security training, however with the rapidly expanding teams as well as remote working coming into play in 2020, something had to change.

By having an engaging, online training platform like Secure Code Warrior, this allowed the Visma team to be able to reach wider and faster to their remote dev teams and ensure that code security was still top priority. This doesn't mean that F2F will be completely eradicated in the future, however it's a great base that can be used as well as interactive in-person training once travel allows.

For Blue Prism it seems that 2020 has simply solidified their beliefs that security needs to be embedded throughout the organization from the beginning. Their strive for technical excellence, putting customers first and developing a product with security at the heart of everything they do, helps them to avoid being the single point of failure not only with their developer security training but across the rest of the organization too.

## How Cybercrime has changed in 2020...

### Do we underestimate the 'bad guys'?

Very much an overall resounding **yes.** Currently, Cybercrime values at more than $1.5 Trillion globally. With many losing their jobs, or pivoting to a new career, cybercrime is seen as something that is a high reward, for little effort. This is showcased by the many scams utilizing COVID-19, pretending to be the NHS or the track and trace application.

Many of these cybercrimes are based on low hanging fruit. A back door, or a mis-configured database. These are the most common, and the ones who can cause a lot of damage for organizations who do not have a security focused culture.

### Are organizations catching up?

Cybercriminals have a head start, whereas organizations who were on prem, and are now having to make the move to cloud due to 2020, are falling behind. It's imperative that those organizations think about their security seriously, and strive for excellence in their technology, not just the essentials.

Some of the best companies who are thriving with their software security are those with the least distance in time between discovered vulnerability and production fix. Those companies are the ones who focus on the best tech, and not just achieving compliance or a tick box.

## Tech Excellence VS Paper Controls

### What's the difference?

The most successful companies are focused on making their technology the best it can be for their customers. This includes security being a part of the quality of code, not an afterthought. Many large organizations who have been around for a while have a large focus on compliance and can often gloss over the importance of security embedded within the culture. Many look at it simply as a tick box. Reviewing documentation to make sure you pass a standard will eventually always come back to haunt you in the long run. By building security in that organization's DNA, it will spread across functions and make the brand and product far more sturdy to cyberattacks, as well as accidental information leakage.

### Security from the ground up, and the top down...

- Every employee should be focused on security, not just the developers or security team. It's important that even your morning barista has security training. Quite often those who are the furthest from the security team are the most at risk, due to lack of education, but still with access to company systems.
- Hire security focused developers. It's extremely important to make sure that the people responsible for the code of your company are interested in security and take it as seriously as they would a feature or function working properly.
- Make it hard for people to make mistakes. Train your developers how to write code securely, avoiding those mistakes in the first place that lead to the low hanging fruit.
- Reward those who are showing interest in security. Create badges, shout them out on Slack, or even just give them a nod in the next team meeting.
- Give the management and board level the type of reporting that helps influence real time decisions. By giving them current, business level security information will help them to prioritize security and emphasize the top down and bottom up approach.

## Key takeaways:

Cybercrime is bigger than ever, which is why it's imperative to make sure that your organization is doing everything it can to do the right thing for your customers.

Whilst compliance is an important business priority, the real impact to a business is to focus on technical excellence, and therefore compliance will follow. This cannot be achieved without producing secure software, and a security culture that goes from the board all the way to your favorite company barista. Secure software can't be solved by a tool (although they help), but by an organization with people who are armed with the right knowledge and have the passion to strive for true technical excellence.