



FLARE

2021 in Review &
**7 Cybersecurity
Predictions for 2022**

Report

<https://flare.systems>

2021 in Review & 7 Cybersecurity Predictions for 2022

The past few years have been monumental in how we interact with technology and how it affects our daily lives. Technology integrated itself in our work and personal lives, enabling us to be more connected and bringing forth a new set of global challenges.

At Flare, we focus on how this ever increasing utility of technology has led to an ever increasing attack surface, a need for contextualized monitoring to provide real time cyber risk assessments, and ultimately we aim to provide accelerated reconnaissance for all organizations.

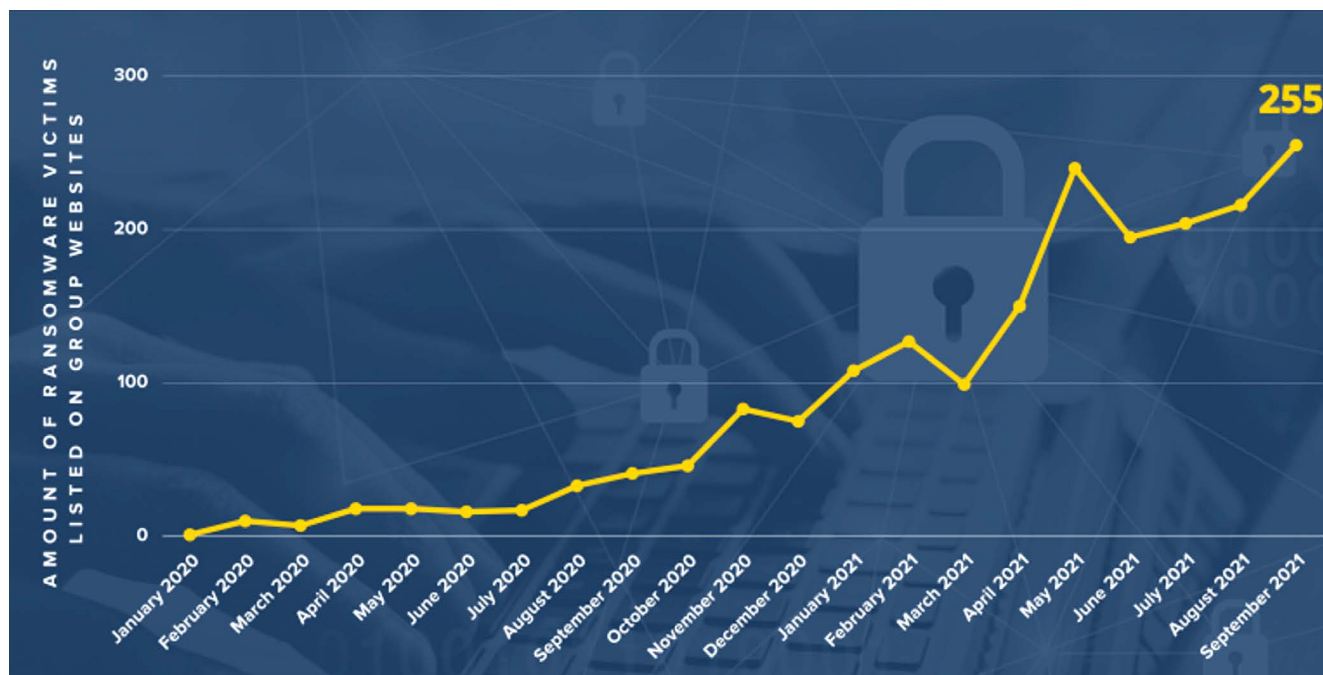
As we communicate with our customers, speak to industry professionals, and gather information from our own experts, we believe there are a few things to note that we'd like to share around the state of cybersecurity in 2021 and will share some of our expert's predictions for 2022.



The Major Cybersecurity Events of 2021 Reviewed

1. Ransomware Increased and Critical Infrastructure Was Successfully Targeted

One of the most frequently discussed cybersecurity topics in 2021 was ransomware.



Flare's primary research on the subject showed a definitive rising pattern in the frequency of ransomware attacks. The rise was exponential. To put it in perspective, [ransomware attacks from 2020 to 2021 increased by 437%](#).

In the past, ransomware seemed to be focused on crypto ransomware and consumers. Today, we see new methods of delivering ransomware and a high level of technology exploitation that has led to an increase in availability and a dramatic rise.

One massive example of ransomware during the year was the Colonial Pipeline ransomware attack. During 2021, we saw an increasing number of successful attacks on core infrastructure which included the colonial pipeline case and other gas, electrical and utilities companies. Additionally we also saw a focus on agriculture and food companies. Due to this, it is clear that in 2021 countries were targeted successfully and not just organizations.

In the past, ransomware has also been focused on the exposing of sensitive data. However, during 2021, we have also seen an increase in ransomware for the cause of disruption. In this case, the malicious actors use ransomware to disrupt company operations and then ask for payment rather than only relying on the threat of leaked data.

2. Data Privacy Became a Competitive Advantage for Organizations

Data leakage and data privacy were also key markers of 2021. Due to the increasing number of cyberattacks, the need for data privacy and awareness among the consumers is rising. A number of large organizations that host a large amount of consumer data were seen to be either misusing data or leaking consumer data. As such, data privacy has become a competitive advantage for companies due to the consumers' new awareness of such issues.

3. The case of the Log4J vulnerability- Log4j Provided a Wakeup Call For Cybersecurity Professionals

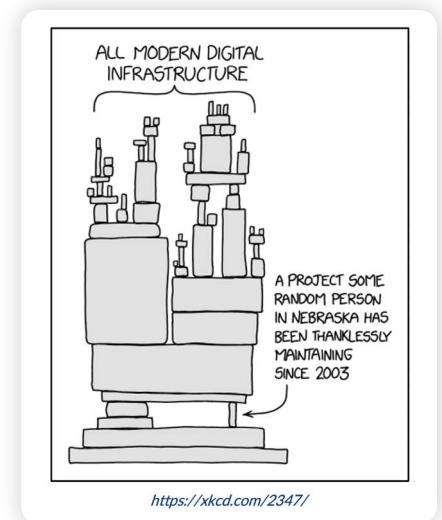
During the end of the year, we saw a massive security issue in the form of the Log4j vulnerability. Log4j and its widespread use caused an uproar in the cybersecurity community as most companies scrambled to patch and address the issue. The vulnerability showcased a clear lack of cohesion in dependency management in turn resulted in many organizations reassessing how they used such open source software.

4. AI Enabled Cybersecurity Professionals with Automation

Lastly, as with any other year, there was the "hot" topic of the season: Artificial Intelligence or AI was still in numerous conversations in our space. One of the most top-of-mind questions any person may ask about AI is, "will AI take my job"? The answer during 2021 was no. AI during the year provided a supplementary position in most cybersecurity teams and proved to be a tool that aided decision making.

That's all from our 2021 in review! Of course, there were many other subjects and areas of discussion, however, to us these were the key aspects we wanted to highlight and believed we could provide some insight on the matter.

In that same lieu, let's now discuss our cybersecurity predictions for 2022!





7 Cyber Risk Predictions for 2022

Prediction 1:

Cyber Criminals Will Continue to Attack Critical Infrastructure

As discussed in our year in review, 2021 saw a considerable rise in successful attacks on critical infrastructure. This increase included attacks on: food Industries, water treatment, utility companies, gas infrastructure, etc. In these specific cases, we can find industrial control systems are being targeted and will continue to be successfully targeted.



According to the Organization of American States and Trend Micro, **“54% of the 500 US critical infrastructure suppliers surveyed had reported attempts to control systems, while 40% had experienced attempts to shut down systems. Over half said that they had noticed an increase in attacks, while three-quarters believed that those attacks were becoming more sophisticated.”**

Research by Lloyd and the University of Cambridge’s Centre for Risk Studies, Business Blackout also suggests that a possible infrastructure cyberattack which causes physical damage to 50 generators which supply power to the northeastern US occurs, Total insured losses are estimated in excess of \$20bn, rising to \$70bn+ in the most extreme version of the scenario. The \$1trn business blackout.

As such we expect not only potential malicious actors to pursue such avenues, but also expect a focus from governments and organizations on how to remediate this threat.

Prediction 2:

Ransomware Will Continue in 2022 But Shift in a New Direction

One of 2022’s biggest cybersecurity issues will be ransomware. However, ransomware may find itself more in the collective consciousness not only through the disclosing of data but more specifically the vulnerability of critical infrastructure.

Through our research, we also predict that ransomware groups will keep changing their approaches and methods. During 2021, we saw the rise of ransomware as a service and saw these groups succeeding in new avenues. If there is one thing that is clear, it’s the fact that these ransomware groups will respond to the new cybersecurity measures that companies and organizations implement. All organizations must take this consideration in mind as we innovate to protect our data, our consumers and our organizations.

Lastly, due to the overall rise in ransomware, cyber insurance itself has become a more contentious prospect. The average insurance payment for ransomware was \$200,000. As the average payment decreases and attacks decrease, it seems that cyber insurance will no longer be worth the price of admission.

Prediction 3:

2022: The Year of Resilience


It is clear that cyber attacks have been increasing, the attack surface is ever expanding and malicious actors are always finding new exploitations. However, we are in agreement with the cybersecurity community and predict that 2022 will be the year of cyber resilience for organizations. How organizations combat existing and future issues will not only affect their stakeholders, but will also showcase their cybersecurity attitude towards its consumers. During this new year, it's not a question of if organizations will face cyber risk more so about how they respond to those cybersecurity issues.

Prediction 4:

A Shift Toward a Zero-Trust Model

In cybersecurity, trust and permissions have been a cornerstone on how organizations protect data. However, recent and past findings still report that most data breaches are caused by human error. A joint study from Stanford University Professor Jeff Hancock, and security firm Tessian revealed that nine in 10 (88%) data breach incidents are caused by employees' mistakes. The study "Psychology of Human Error" highlighted that employees are unwilling to admit to their mistakes if organizations judge them severely.

Due to the prevalence of this phenomenon, companies are beginning to adopt a more comprehensive permissions methodology called the zero-trust model. In this model, companies give and will give only the right amount of data access to their employees to minimize the potential of human error and its damage. Organizations implement such a model to ensure that only the right information is with the right person at the right time.




...88% of data breach incidents are caused by employees' mistakes.

Prediction 5:

2022: The Year of Privacy

Data breaches, data leaks and the overstepping of many technology organizations have made consumers very wary of who has their data and how it is being protected.



...60% felt their country's privacy laws have a positive impact...

On the subject of data privacy, Cisco released a 2021 Consumer Privacy Survey, which draws on 2600 anonymous responses across 12 countries. The report found that nearly half of survey respondents felt that they were unable to protect their personal data and the top reason cited is that companies aren't being clear about how they are using this data. One third of consumers also reported becoming "privacy actives", which includes individuals that switched companies or providers over their data practices. This firstly showcases that consumers want transparency and control of their data.

However many consumers are not aware of specifics of their data. According to the Cisco report, 60% felt their country's privacy laws have a positive impact, versus only 4% who said they are having a negative impact. However, only 43% overall are aware of these laws. Awareness varies significantly by country, from 25% in Japan to 70% in India. Flare predicts that this awareness will only increase and consumers will start to look for privacy as a feature and it will become a competitive advantage for organizations.

Flare predicts that the need for data security and privacy will also become a more pertinent compliance matter. During 2021, here are all the laws that passed that concerned themselves with data privacy:

- The Colorado Privacy Act (ColoPA) and the Virginia Consumer Data Protection Act (VCDPA) advanced into law (with effective dates of 2023);
- China's Personal Information Protection Law took effect;
- The UAE released its new privacy law;
- South Africa's privacy law came online;
- California voters passed the California Privacy Rights Act (CPRA);

If 2021 is an indication, 2022 will showcase a greater focus on passing laws that comply with organizations to more effectively protect data and ensure the privacy of its consumers and employees.

Prediction 6:

Dependency Management Software Is Going to Improve

Log4j caused massive security issues as soon as the vulnerability was known by the public. However, Log4j showcased a more systemic issue in dependencies management. Log4j was and will continue to be a wakeup call for the industry.

When Log4j occurred one of the issues most companies faced was the question of where to even start to address the issue. Log4j ran in databases, legacy software, and anything that ran in Javascript was affected. Due to this massive variability, companies found it difficult to understand where to start and to what extent the issue was present.

Everything is now moving to containerized applications. The consequence is that, now, patching bugs of this nature is much harder than it was a couple of years ago because it's running in twelve different containers on the same machine. It's running on applications where you don't even necessarily control the build system. Just knowing what apps you're running that are affected is also challenging because you need to have good dependency management tooling to know that it's running inside that specific container on that specific machine. This is where dependency management becomes really important. Only knowing that you have the database running and its specific version is no longer enough.



Prediction 7:

Real AI Will Be More and More Used in Cybersecurity

AI will continue to expand its role in cybersecurity in 2022, and will not replace your cybersecurity team. According to Forbes, AI is currently used and will increase in use in three key avenues:



Network Vulnerability Surveillance and Threat Detection

AI can and will be used to accelerate reconnaissance on cyber threats. Currently, there are numerous softwares and platforms that monitor real time activities on networks by scanning data and files to recognize:

- Unauthorized communication attempts
- Unauthorized connections
- Abnormal/malicious credential use
- Brute force login attempts
- Unusual data movement
- Data exfiltration

Businesses then use this data to infer threats through anomaly detection.



Incident Diagnosis and Response

Incident analysis software can discover vulnerabilities and provide insight on the severity of such exposures. Once the causes of an incident are identified, prescriptive analytics can be leveraged to respond to the incident based on recommendations to contain and eradicate the causes of the incident permanently. These recommendations can cover a wide range of applications varying from taking specific actions, change in strategy, and adoption of new procedures or processes.



Cyber Threat Intelligence Reports

Lastly, cyber threat intelligence reports are and will be used to help understaffed cybersecurity teams around the world collect, organize, analyze and proprotize data. The information can be compiled and summarized or even be the subject of a report fully written by an AI program through natural language processing. Cyber threat intelligence reports provide the indicators and early warning necessary to better monitor unusual activities on a given network and detect more rapidly cyber threats.

According to Meticulous Research, the market of artificial intelligence in cybersecurity is expected to grow at a compound annual growth rate of 23.6% from 2020 to 2027 to reach \$46.3 billion by 2027. It is clear that the avenues in which AI can help are numerous, however, AI can also be used by malicious actors to combat organizational AI. In the end we predict that organizations will further adopt AI to help their cybersecurity professionals face cyber risks in the future.

About Flare Systems

Since 2017, Flare Systems has been developing AI-driven technologies to protect your companies against malicious actors and human errors. Firework offers an easy-to-use platform that gets you the right information before risks become unmanageable. Reduce digital risk and fraud with Firework, the digital risk protection (DRP) platform that automates your dark, deep and clear web monitoring to deliver real-time actionable intelligence.

David Héту is a co-founder and Chief Research Officer of Flare Systems. David has a Ph.D. in criminology from the Université de Montréal. His main research interest is in online illicit markets and the impact of technology on crime, whether it be from the offenders' point of view or from a regulation point of view. David's research has been published in the highest academic journals (ex. British Medical Journal) and presented at leading conferences (Botconf, HOPE). He is regularly invited to share his analysis of cybercrime in media outlets. David has developed the DATACRYPTO software tool to monitor darknet activities and has co-developed the BitCluster software tool.

Luana Pascu is a cybersecurity writer and researcher at Flare Systems. Luana has a MA in New Media from the University of Amsterdam and a MA in Marketing from the Academy of Economic Studies in Bucharest. For over six years, Luana's work has been focused on discussing cybersecurity, IoT, data privacy and biometric security. Luana is a supporter of women in tech and has a passion for entrepreneurship, technology, and startup culture.

[Free Trial](#)

[Book a Demo](#)

www.flare.systems
hello@flare.systems



1751 Rue Richardson, Unit 3.107
Montreal, Quebec, H3K 1G6