



# Cybersecurity 2020-2021:

trends and forecasts

[ptsecurity.com](https://ptsecurity.com)

**Contents:**

Illuminating with facts, figures, and new ideas	3
The Great Siege of 2020	4
Governments	7
Attacks on users	8
Attacks on the industrial sector	9
Security of telecommunication networks	11
Security of the financial sector	12
Hardware vulnerabilities	16
Mobile security	17
Security and AI	18

## **Illuminating with facts, figures, and new ideas**

Information security is shaping the agenda like never before. And rightfully so: the number of threats and cybercriminals is growing every year. Management at many companies has become more responsive to cybersecurity issues. They realize that certain business risks must simply be stopped, no matter what. Of course, committing to such real-world security comes at a financial cost.

Businesses saw that 2021 would be quite different in terms of IT and security budgets. Therefore, they tried to make the most out of their existing plans and leverage all the resources they could bring to bear.

### **COVID-19 still impacting business outlooks**

The COVID-19 pandemic has certainly affected the cybersecurity market. However, the practical impact has not been as much as feared. In late Q1 2020, the situation was precarious as the number of pilot projects dropped significantly. The reason was obvious: lockdowns and the rapid transition to remote work made such projects more difficult or even impossible to implement on companies' premises. At the same time, the new realities underscored the importance of not stopping ongoing cybersecurity efforts. Together, these two factors created a rather dangerous dynamic, in which companies might skip pilot deployments (despite their importance for making an informed choice) and instead simply choose the lowest bidder no matter what. Fortunately, these fears did not materialize. Competition on the domestic infosec market remained strong and the demand for security that works kept companies from taking the easy way out when it came to choosing protection tools.

### **Opting for real information security**

As we have mentioned before, the security paradigm itself is changing. The infosec community has moved away from the idea of building moats. No matter how good a security system is, getting hacked is a matter of "when," not "if." That's why these days, the goal is to detect an attacker inside the network as soon as possible. The ability to detect is the crucial thing, in other words. However, over the last year, this concept evolved. We now see that it is possible to create a security system guaranteeing that attackers will not be able to actuate specific business risks. We still agree that any company can be hacked, but the goal of information security can and should be to keep attackers from causing any significant harm. This trend took shape quite recently, just in the last year, and will likely dominate in the years to come. It will be vital to create a new type of security operations center (SOC). Instead of being measured by 24/7 availability or the speed of incident response, these results-oriented SOCs will be subject to an SLA-like arrangement centered on the ability to stop attackers from triggering unacceptable risks. Such SOCs will be judged on a "pass/fail" scale: was a risk triggered, or not? Cyberexercises become essential, as they are the only way (short of a real incident) to measure how well the security system and SOC work. Vague checklist-like assessments are all too common. Only

properly organized cyberexercises can cut through the window dressing to provide actionable results.

This approach should ultimately expand the market and make a real difference by keeping only the solutions and technologies that work. This is Darwin's theory in action: only technologies able to quickly detect attackers, block them from pivoting and escalating, and throw them off of infrastructure entirely, will survive. As a vendor, we are already working on an automated smart solution to accomplish these tasks quickly and efficiently.



### Alexey Novikov

Director of the Positive  
Technologies Expert Security  
Center (PT ESC)

## The Great Siege of 2020

The massive shift to remote work gave rise to new information security risks. Social engineering became a common method for penetrating companies' networks. All types of hacker groups took advantage of the pandemic. COVID-19 fueled both mass campaigns and targeted ones. As we predicted in 2019, the number of advanced persistent threat (APT) attacks kept growing in 2020.

Throughout the year, we monitored around 30 APT groups. Attribution is becoming more and more difficult, since hackers often combine various malware tools normally attributed to different gangs in a single attack. When we report to companies that they have been hacked by an APT group, all too often this news comes as a surprise to them. In 2020, PT ESC performed 47 investigations.

2020 showed that insiders still present an acute risk for companies, as proved by the [incident at Tesla](#). People constantly communicate via social media and chat, and it is getting ever more important to protect these platforms. A notable example is the [mass hijacking of celebrities' and politicians' Twitter accounts](#).

Ransomware was a major headache in 2020. The ransoms for decryption were huge, and when victims refused to pay, attackers published the data on the web. Some companies had to stop operations for several days. One prominent example was the [cyberattack on Garmin](#). We discussed the increase in ransomware and other destructive attacks back in 2017. Not only financially motivated hackers are encrypting entire infrastructures: [APT groups have joined in as well](#).

### Supply chain attacks

We warned back in 2017 about supply chain attacks, and in 2020 they caused plenty of headache. By now everyone has probably heard of [what happened with SolarWinds](#). Our company has come across similar attacks on software vendors, security developers, IT integrators, IT contractors, and government websites in a number of countries. Security at large companies is improving, which makes them difficult targets, particularly for attackers interested in long-term persistence and not just a one-time hack. That is why APT groups are turning their sights to the partners and contractors of such companies. Only top-tier security experts are capable of protecting from such attacks.

## Forecasts

In 2021, we expect hackers to refine social engineering methods for taking advantage of current events, especially COVID-19. We also anticipate that phishing attacks will become more tailored, with use of instant messaging and social media to make contact with victims. To overcome corporate protection systems, attackers will try to hack personal computers of employees.

In 2020, many APT attacks targeted pharmaceutical companies, including vaccine development laboratories. The virus is mutating and research is ongoing, which means that hackers will stay interested in these companies for the foreseeable future. We also expect APT attacks to keep climbing in 2021.

Groups such as APT 27 are increasingly using ransomware in targeted attacks. In 2021, we expect that such attacks will grow.

We will probably see supply chain attacks similar to the SolarWinds hack, as well as more attacks on IT and infosec companies and cloud infrastructures.

We recommend that all companies get to know their infrastructure in detail, quickly respond to any anomalies, and keep an eye on network entry points used by remote workers. As a minimum, the starting point for security-minded companies should include antivirus software, SIEM, NTA, and a web application firewall (WAF).

## The flip side of working from home: attacks on remote desktops and collaboration software

COVID-19 and the shift to remote work led to a worldwide rise in attacks on web-accessible corporate services. Companies had to urgently push their services to the perimeter. Because of the large number of people working from home for the first time, more corporate hosts became accessible for RDP connections. As a result, the share of attacks exploiting software vulnerabilities and configuration flaws increased to 36 percent in Q4 (compared to 9% in Q1).

From quarter to quarter, we saw an increase in malware attacks with exploitation of vulnerabilities on the network perimeter. Attackers actively exploited vulnerabilities in VPN solutions and remote access systems, such as those from Pulse Secure, Fortinet, Palo Alto, and Citrix. They also looked for vulnerabilities in web applications and bruteforced RDP passwords.

Another pandemic-related trend is the theft of credentials for audio- and videoconferencing services, such as Skype, Webex, and Zoom, as well as tampering with these conferences.

In 2020, criminals pursued a wide range of goals, from cryptocurrency mining to cyberespionage against large companies. They have multiple types of malware at the ready and increasingly use multifunctional trojans or plant a wide array of malware on compromised devices. Malware operators can transfer access to infected devices to other criminals. Malware itself is evolving in the direction of greater stealth and evasion capability against antivirus and protection software, including sandboxes. New functionality and exploits for new vulnerabilities are being added as well.

## Ransomware booming

In 2020, we saw a constant increase in ransomware attacks. In Q1, ransomware accounted for 34 percent of malware attacks on organizations. In Q4, it reached 56 percent. Mass ransomware attacks became less common. Malware operators are deliberately choosing large companies that have deep pockets or for which downtime could be catastrophic. Once the target is chosen, hackers strike.

Ransomware is one of the fastest-growing varieties of cybercrime. It has become a common practice for attackers to threaten to disclose the stolen data unless the victim pays a ransom. Maze, Sodinokibi, DoppelPaymer, NetWalker, Ako, Nefilim, and Clop operators were the most active perpetrators of such attacks in 2020. Some of them even implemented a "double extortion" scheme by demanding separate ransoms for decryption and non-disclosure of data. To sell the stolen data, many ransomware operators create special websites where they publish a list of victims and the stolen data. They may even auction it off. There are ransomware alliances that publish stolen data as part of partnership agreements.

## Access for sale, ransom for non-disclosure

Other criminals have quickly caught up with the trend of demanding ransom for non-disclosure of data. For example, hackers can demand a ransom from online stores by threatening to sell the stolen data to third parties. Compared to ransomware operators who demand millions of dollars as a ransom, their appetites are more modest, on the order of \$500. Nevertheless, this business model can offer significant profits: database owners are often willing to pay to protect their reputation, while the criminals never run out of potential buyers.

Attackers sometimes buy access to companies' networks from other criminals. Ransomware operators were among the first to use this scheme. They propose cooperation, recruit affiliates to spread ransomware, and share a percentage of any ransom received. On the darknet, this access-for-sale scheme allows even low-skilled hackers to earn money. All they need to do is find vulnerabilities on external resources of the victim company and sell this information.

## Forecasts

In late 2020, we saw a slowdown in the explosive growth in attacker activity that had accompanied the beginning of the COVID-19 pandemic in the first two quarters of the year. But the number of attacks remains persistently high and quarter-over-quarter growth in the number of incidents continues.

We expect to see new criminals motivated by high ransomware profits. These will include malware operators and those who provide access to victim infrastructure in return for a percentage of the ransom. We will likely see new cybergroups and platforms for selling stolen data. Ransomware owners will likely keep the blackmail strategy, honed in 2020, of demanding separate ransoms for infrastructure recovery and non-disclosure of stolen data. However, even without taking into account ransom payments, ransomware attacks come at a high cost, including system recovery, downtime,

possible loss of clients, and other consequences. For example, IT service provider Sopra Steria estimated losses as high as €40-50 million due to a Ryuk ransomware attack on the company in October 2020.

Most companies continue to work remotely, either partially or fully, which means that attackers keep looking for any security lapses in systems on the network perimeter. At the same time, the rise of access-for-sale on the darkweb makes companies, including large ones, a target for low-skilled hackers eager to make a fast buck. External attacks on corporate infrastructures will continue to grow. That is why companies need to assess the security of their network perimeter, take an inventory of externally accessible resources, and build an effective vulnerability management process.

### But there is also good news

Many companies have learned to accommodate remote work. In early 2020, they had to rapidly shift employees to working from home. In 2021, they can correct past mistakes by allocating budgets for protection tools and implementing best practices.

Companies can no longer ignore the risks. They want to measure the real consequences of possible cyberattacks and, when an attack does take place, minimize negative outcomes. A number of platforms now offer the ability to conduct training and exercises. The most effective cyberexercises use digital models to re-create real corporate infrastructures. Use of cyber-ranges to model business risks will become a driving trend in information security.

## Governments

Government institutions remain the most attractive targets for hackers, receiving 19 percent of all attacks on organizations. In 2020, we recorded 359 attacks on such targets. Compared to 2019, these attacks were significantly more likely to involve malware (71%) and social engineering (64%). The pandemic may have been a factor: many attackers sent emails to governments in various countries with malicious attachments that preyed on the coronavirus situation. Cyberespionage attacks accounted for 58 percent of cases.

In early 2020, our experts observed phishing attacks by APT groups [SongXY](#), [APT36](#), [TA428](#), [TA505](#), and [Higaisa](#), in which they spread malicious documents with pretexts related to COVID-19. The pandemic was also leveraged in attacks with Chinoxy and KONNI malware. Throughout 2020, the Positive Technologies Expert Security Center recorded attacks by the Gamaredon group targeting government institutions in Ukraine and Georgia.

### Forecasts

Many government services have become available online for the first time. Even elections can now be held electronically. The pandemic, with resulting lockdowns and monitoring, has driven governments to use technology like never before. As new electronic services appear, they will inevitably attract criminals and require special attention with regard to information security.

## Attacks on users

In 2020, we recorded 325 campaigns against individuals. The number of such attacks increased by 11 percent compared to 2019. In most cases (93% of attacks), ordinary users become victims of mass campaigns. Most times, attackers used social engineering (69% of attacks). In 59 percent of attacks, hackers infected user devices with malware. In most cases, they spread malware via websites, email, and official app stores. Half of malware attacks against individuals involved spyware, and in 22 percent of cases attackers used banking trojans. Attacks were mostly driven by theft of credentials. Credentials accounted for 36 percent of all stolen data, followed by personal data and payment card information (19% each).

COVID-19 phishing attacks mostly affected ordinary users. Techniques went beyond just malicious emails. Attackers also hosted malware on fake pandemic-themed websites and distributed malicious mobile apps. At the beginning of the pandemic, criminals lured their victims with personal protective equipment or additional information about the virus. More recently, they have started playing the vaccine card.

In the first half of 2020, many companies shifted their employees to work from home. Criminals took advantage by using individuals as a stepping-stone for access to corporate targets. People are often unaware of basic security rules or neglect them when working from home, which places them and their employers at greater risk. Lack of software updates, unlicensed software, old OS versions that are no longer supported, lack of antivirus software, use of weak passwords, and other gaps on personal computers can all give attackers a way in to corporate networks.

### Forecasts

The pandemic will remain a tool for spreading malware as well as stealing money and card numbers from ordinary users. Possibilities for fraud include websites purporting to offer COVID-19 treatments, paid vaccinations, or vaccination certificates. Phishing messages will disguise malware as information about vaccinations, related timeframes, or so-called vaccine passports.

The UEFA European Football Championship is another likely topic for social engineering attacks. Such large events tend to inspire fake websites aimed at stealing data and money.

Magecart-like attacks will continue targeting online stores and other merchants. In these attacks, malicious scripts are injected into the websites of hacked companies. These scripts collect all data entered by website users—including, of course, payment card information. These techniques are highly effective because the security of web applications is often neglected. In many cases, attackers can simply leverage known vulnerabilities in popular content management system (CMS) software. But ordinary web visitors are the victims.





**Dmitry Darensky**

Head of Industrial  
Cybersecurity Practice  
at Positive Technologies

## Attacks on the industrial sector

2020 saw an increase in attacks against industrial and energy companies. We recorded 239 attacks on such companies, which represents an increase of 91 percent over 2019 (125 attacks). In nine out of ten cases, attackers used malware. Ransomware and spyware were present in 41 and 25 percent of malware attacks, respectively.

Attackers sent phishing emails to spread malware and gain a foothold on local networks. They also exploited vulnerabilities on the network perimeter.

In most cases, industrial companies were attacked by ransomware operators and APT groups. One out of six ransomware attacks against organizations was aimed at the industrial sector. At the beginning of the year, many cybersecurity experts turned their attention to the new ransomware called Snake, capable of deleting shadow copies and stopping industrial control system (ICS) processes. Snake can stop such processes as GE Proficy and GE Fanuc Licensing, Honeywell HMIWeb, FLEXNet Licensing Service, Sentinel HASP License Manager, and ThingWorx Industrial Connectivity Suite. The first victims of the Snake ransomware were automaker Honda and energy giant Enel Group. Throughout the year, industrial companies were also struck by other ransomware operators, including Maze, Sodinokibi, Ryuk, NetWalker, Nefilim, DoppelPaymer, RansomEXX, and Conti.

The industrial sector is targeted by many APT groups worldwide. For instance, one APT attack by the Bisonal group in Q1 2020 targeted Russian aerospace organizations. Attacks by the RTM group continue at a high pace in Russia and the CIS countries: PT ESC detected over 100 malicious mailings by the group in 2020.

## Forecasts

Since the beginning of 2021, the number of attacks against industrial companies has increased and remained consistently high. We do not expect that attackers will lose interest anytime soon. The main motive will not only be espionage, but also the possibility to receive large ransoms in return for data recovery and non-disclosure of stolen information.

News reports of an industrial company stopping operations due to a cyber-attack used to be rare. There were two reasons. For one thing, companies wanted to hush up such incidents. And for another, they often could not determine whether the disruption was actually the result of a cyberattack or something else. But today, hacks of major energy and industrial companies are a frequent occurrence. Most often this takes the form of a targeted ransomware attack. These attacks are difficult to hide, and the culprit is obvious: the criminals themselves inform of the hack by way of demanding a ransom.

All this shows an extremely low level of protection against external threats, plus the inability to detect and stop attackers in a timely way. One can only guess how many spyware campaigns remain undetected and undisclosed. Criminals will likely continue pursuing these victims, with a preference for large companies. At the same time, they will try to minimize the outlays necessary for performing a hack or purchasing access from other criminals. Data leaks and disruptions at industrial companies are a sure bet for 2021.

Ransoms will also likely increase. They already reach tens of millions of dollars in some cases, and the more companies fall victim to attacks, the more motivated hackers are to go on. We also expect to see new attacker groups and cooperation among criminals to make money off security vulnerabilities at industrial companies.

At the same time, on top of ensuring formal compliance with regulatory requirements, industrial companies are busy working to secure their assets in real-world ways. The following trends will be relevant in 2021:

1. **Risk-oriented threat modeling.** Industrial companies will start understanding digital security risks in a more rigorous and meaningful way. Instead of classic probabilistic methods that look only at individual systems or components, the new approach places cyberthreats in a risk context at the operational and business-wide level.
2. **SCADA data-driven anomaly detection and response.** Companies with ICS infrastructure are analyzing SCADA data to spot anomalies and attacks. This trend will be especially pronounced on NTA/NDR, EDR, and SIEM systems.
3. **Automation of security management processes.** Security management processes, especially for detection and incident response, are becoming increasingly automated.
4. **Digital twins and cyber-ranges.** Modeling of virtual copies ("digital twins") of industrial systems is coming into its own as a way to study ICS vulnerabilities and emulate attacks. At cyber-ranges, companies can safely use this method to test the feasibility of business risks and analyze potential attack methods.

### The Standoff: successful attacks without real consequences

Digital modeling offers unique capabilities for understanding cyberattacks on information infrastructure. Participants at The Standoff cyber-range have the run of the same real equipment and software used at industrial companies and can verify the feasibility of various risks in practice. At The Standoff in November 2020, red teams pulled off several attacks on a petrochemical plant and an oil refinery. In real life, such attacks would have caused enormous damage. Attackers gained access to the plant management system, which allowed them to disrupt and completely halt the production process. The resulting modeled accident released toxic substances. At the virtual oil field, attackers disrupted oil extraction machinery. In addition, hackers gained access to the oil storage management system and disrupted pumping to oil terminals. Later, they also halted the petroleum transport controller. It takes a cyber-range to truly model these risks in full. Attempting such experiments as part of penetration testing or cyberexercises would have damaged equipment, forcing companies to settle for the ability to demonstrate only to a certain point. The cyber-range, however, allowed finishing the attack and assessing the real consequences.



**Pavel Novikov**

Head of Telecom Security  
Research at Positive  
Technologies

## Security of telecommunication networks

The main security challenge for telecom systems consists of the vulnerable protocols used in 2G, 3G, and 4G networks. For example, SS7 vulnerabilities in 2G and 3G networks allow all sorts of attacks, from information disclosure to SMS interception, eavesdropping, and disruption of subscriber service. The Diameter protocol in 4G networks has vulnerabilities that allow tracking subscriber geolocation, bypassing operator blocks, and causing denial of service. Flaws in the GTP protocol allow attackers to interfere with network equipment and leave an entire city without communication, impersonate users to access various resources, and use network services at the expense of the operator or subscribers.

Moreover, all these security issues remain relevant for 5G Non-Standalone networks, which are built on the infrastructure of previous-generation networks. Just like 4G, most 5G networks are vulnerable to disclosure of subscriber information (including geolocation data), spoofing (such as for fraud), and DoS attacks on network equipment, resulting in mass disruption of mobile service.

As for 5G Standalone (5G SA) networks, we can say that despite all the protections present in the HTTP/2 protocol (the successor to SS7 and Diameter in 5G SA), attackers can still spoof or remove network elements, which can lead to network malfunction. In addition, with access to internal interfaces, attackers can perform DoS against subscribers and intercept incoming traffic by exploiting vulnerabilities in the PFCP protocol (the 5G SA successor to GTP-C).

Denial of service is a serious threat to IoT devices. These devices, which are becoming the main "subscribers" of mobile operators, are key to the functioning of smart homes as well as the urban and industrial infrastructures in which they are embedded.

Mobile operators are aware of the threats but rarely take a systematic approach to security. As a result, even when expensive niche solutions are installed, networks still tend to be poorly protected in practice.

### Forecasts

The vast majority of people will still be served by 2G, 3G, and 4G networks, which means that all the "old" vulnerabilities will be as important as ever. Many operators are starting 5G SA deployment in 2021, but full-fledged commercial rollouts will be slower in coming. The insecurities of 2G, 3G, and 4G networks will still be with us for a while. What's more, 5G networks interwork with other mobile networks. Hackers can perform cross-protocol attacks by exploiting vulnerabilities in multiple protocols as part of a single attack. For example, an attack on 5G might begin with exploiting 3G vulnerabilities to obtain subscriber identifiers. That is why protecting previous-generation networks is essential for 5G security.

Researchers continue to investigate the 5G architecture and protocols, searching for vulnerabilities and flaws. Even though the specification developers took into account the security flaws of previous-generation mobile networks, new technologies come with new risks.



**Maxim Kostikov**

Head of Banking Security  
at Positive Technologies

Nor will GTP security issues go away completely, even after the transition to 5G Standalone. GTP is planned for use on Standalone networks, too, including roaming, even if only to transmit user data over the GTP-U protocol. Attacks on GTP-U allow encapsulating management protocol packets in user sessions or obtaining data about subscriber connections. This is why, when 5G SA networks arrive, additional research will be required to see whether the new management protocols remain vulnerable.

## Security of the financial sector

In 2020, we recorded 126 attacks against financial companies, compared to 92 in 2019. Phishing factored into 61 percent of attacks. It remains the main method for breaching the local networks of financial companies. Hacking (defined as exploitation of software vulnerabilities and flaws) figured in 21 percent of cases. Malware was present in 65 percent of attacks. The most common malware types were spyware (28% of malware attacks), ransomware (29%), and banking trojans (23%). Ransomware attacks against financial institutions increased, just like in other sectors.

According to the Positive Technologies Expert Security Center, the RTM group kept attacking financial organizations with malicious emails throughout the year. During the first two quarters of 2020, our experts recorded phishing attacks by the Cobalt group.

The European Association for Secure Transactions (EAST) has reported an increase in ATM logical attacks in Europe. All the attacks reported in the first half of 2020 were black-box attacks.

### Forecasts

No new major hacking groups specialized in withdrawing money from bank accounts appeared in 2020, nor are any more expected to appear in 2021. Attacks on small banks are less profitable than targeted ransomware attacks. In addition, they are much more difficult to perform, since they require specialized knowledge of banking processes and software. We will most likely encounter attacks by known groups that conceal their attacks by using multiple techniques for penetrating and gaining persistence, refine their malware, and vary the regions they target.

We may expect an increase in ransomware attacks on banks. Such attacks have become a common practice, pay off well, and do not involve any extra costs. Attackers will keep searching for known vulnerabilities on the perimeter to spread malware. Our penetration tests at financial institutions demonstrate a low level of security: at seven out of eight companies, real attackers would have been able to penetrate local networks from the Internet.

### Key issues with ATM security

Banks are actively upgrading their ATMs to Windows 10. It has more features than previous versions, which means that attackers have more options for bypassing kiosk mode and gaining access to the operating system.

Our experience shows that ATMs do not securely implement software access control. Attackers can execute arbitrary code after gaining access to

the OS and tampering with executable files on the device. With this code, they can dispense cash or steal personal data.

Black-box attacks remain a major concern, as they can lead to ATM cash thefts. Banks are considering whether to implement authentication of ATM-connected devices (such as USB flash drives and keyboards), which should significantly reduce the risk of attacks and kiosk mode bypasses.

As for network security, we have noticed an improvement in network policies and the use of VPNs to protect ATMs. However, not all banks have taken these steps. This absence enables attackers to tamper with traffic between the ATM and processing center. Results include theft of sensitive information or withdrawal of funds. In addition, traffic inside the VPN is often not protected with additional encryption, making it vulnerable to an insider.

### Security of banking web applications

In 2020, the security of banking web apps took a turn for the better. The number of standard web vulnerabilities (XSS, SQLi, and RCE) decreased, and the transition towards a microservice architecture enhanced system resiliency. The bad news is the increasing number of logical vulnerabilities that may allow attackers to steal money and user data and perform denial of service attacks. Instead of trying to fully compromise banking web apps, attackers are focusing on vulnerabilities in application logic in order to:

- Get a more advantageous exchange rate, transfer funds from client accounts, or avoid fees.
- Obtain as much information about bank clients as possible for social engineering attacks.
- Overload the system and cause denial of service.

We expect banks to pay more attention to eliminating logical vulnerabilities in 2021.

### Security of banking infrastructure

Financial institutions are still poorly protected from APT attacks. Attackers are successfully actuating the most dangerous business risks by accessing bank workstations, ATM management systems, and card processing systems. In 2020, Positive Technologies pentesters regularly helped banks to verify business risks by emulating attacker actions, and each time they were successful (with an average of three to five business risks confirmed at each bank).

When the internal attacker model was used, our pentesters managed to obtain maximum privileges on infrastructure in 100 percent of cases and demonstrate the feasibility of business risks. These risks refer to unacceptable events defined jointly with our clients in advance, such as unauthorized access to critical systems, including bank workstations, SWIFT terminals, ATM network, and processing center, depending on the particular bank.

In some cases, our experts did not act as internal attackers. Instead, they used the external attacker model, in which a pentester does not have pre-existing access or any privileges on the tested systems—just a “person

off the street.” Yet even in these cases, our testers still managed to breach the perimeter, obtain maximum privileges, and trigger key business risks.

## Problems of new financial technologies

Modern financial technologies—hyperlinked payments, QR codes, digital currencies, biometrics, and the latest web technologies—all have their advantages and disadvantages.

### Anti-fraud flaws

Automation errors and related risks are the bane of modern anti-fraud solutions. Algorithms designed to spot unusual transactions can sometimes flag legitimate purchases by accident. Widespread automation, aided by big data, should reduce false positives and let legitimate payments go through. But eliminating false positives entirely will be a tall order.

The more banks try to protect their clients, the more inconvenience they are liable to cause. Any automated system has to make trade-offs. An algorithm for identifying fraudulent transactions can be strict, which will catch more suspicious transactions but also block legitimate payments more often. Conversely, a “looser” algorithm reduces client hassle but will leave more fraudulent payments undetected. The challenge will be to find the delicate balance between security, frictionless convenience, and business requirements.

### Blockchain risks

Blockchains, as a distributed ledger that makes payments transparent at every step, have the potential to streamline the payment process. In such systems, the weakest point is client access to the payment system and digital wallet itself. Even a supersecure blockchain cannot stop hacks that target a web interface or the client’s device.

Businesses are curious about smart contracts—instead of a wall of legal text, they comprise a self-executing algorithm that automatically verifies whether each side has fulfilled its obligations. However, these algorithms are written by people, and people make mistakes. The code of a smart contract can have errors and even backdoors, which opens a new chapter in the history of financial fraud. Having the text of an agreement contain “vulnerabilities” is a new problem for the industry. Learning how to find such vulnerabilities in smart contracts and preventing related types of fraud will be vital.

Distributed ledgers also have implications for fraud. Rolling back a single ledger transaction is not possible because this would also affect legitimate transactions that happened to be occurring at the same time. Authenticating transactions is key for digital currencies, which is why each transaction must be signed cryptographically. At the national level, it will become important to implement domestically devised cryptographic algorithms in the software used for digital money and smart contracts.

Businesses and regulators should combine efforts to facilitate successful implementation of smart contracts and distributed ledgers. Doing so will take effort and commitment.

### Mobile phones and money

Reliance on mobile phones carries additional risks. Perhaps the most obvious of these is SIM swapping, in which a fraudster impersonates a bank client to obtain a "replacement" SIM card in order to change the password for the client's bank account. Another is exploitation of vulnerabilities in financial applications, which make it possible to link any phone number to an attacker-specified account. Funds sent to that phone number will then be received by the attacker. And attackers keep inventing new techniques all the time.

Biometric identification is becoming popular, but also creates serious risks. Iris and fingerprint recognition are regarded as highly reliable, for example, thanks to their low error rate. However, these are not the same biometric methods used for remote identification, such as facial recognition and voice recordings. Those methods are not nearly as reliable. Attackers could use deepfakes to automatically generate images and voices that successfully pass biometric identification.

Moreover, practice shows that even robust identification will not stop attackers, who instead bypass such mechanisms entirely by taking advantage of social engineering or vulnerabilities in payment applications.

Unfortunately, many initiatives by the banking sector to limit fraud, such as creating a central database of SIM cards or placing per-transaction limits on rapid payments, have received pushback from clients. Overcoming this attitude and teaching users basic digital hygiene will be a serious challenge for the banking community around the world in coming years.

### Cyber-ranges: stresstesting bank security

Simulated cyberattacks at [The Standoff](#) in November 2020 tested the security of digital replicas of the infrastructure of real companies. Among the companies modeled on the cyber-range was a digital bank. Attackers tried their hand at triggering a number of business risks: disrupting transaction processing, stealing money from client bank accounts or cards, and stealing personal data of bank employees and clients. As a result, the attackers triggered half of the total designated risks: they transferred money from client cards to attacker-controlled accounts and obtained access to personal data of bank employees and online banking clients. Almost all attacks (except one attack conducted in the closing minutes of the contest) were detected and investigated by defenders. The Standoff is an ideal opportunity for security specialists to gain experience and boost their professional skills.

The business risks modeled at The Standoff are highly relevant to financial organizations. In penetration tests at financial organizations, our experts managed to obtain maximum privileges on corporate infrastructure in 100 percent of cases. In some cases, the experts also checked whether potential attackers would be able to steal funds; all such attempts were successful. Security assessments of mobile banking systems also revealed security problems: in half of mobile banking apps, hackers could perform fraud and steal money.



**Alexander Popov**

Lead OS and Hardware  
Security Researcher at  
Positive Technologies

## Security of operating systems

2020 was very productive for operating system security. A number of important developments made for an eventful year. Fortunately, the pessimists were wrong and the pandemic did not slow down the development of system software. In their annual reports, both the [Linux Foundation](#) and [GitHub](#) even noted growing open-source engagement.

Operating system security continues to be an important area for innovation. There can be no easy one-size-fits-all solutions. Thoughtful and comprehensive approaches are required. Three main vectors point the way forward for improving the security of operating systems.

One: secure processes for software development. The operating system cannot be secure if the development process does not include cross-review, fuzzing, static analysis, and control over the software supply chain.

Two: developing and implementing OS mechanisms that increase the difficulty of vulnerability exploitation. If an attacker wants to exploit an error in the OS kernel, we can frustrate that attempt as much as possible.

And three: new hardware technologies for eliminating entire classes of OS vulnerabilities. These tools include ARM Pointer Authentication Code (PAC), ARM Memory Tagging Extension (MTE), and Intel Control-flow Enforcement Technology (CET). The relationships between these and other technologies, vulnerability classes, and exploitation techniques can be seen in the [Linux Kernel Defence Map](#) that I have developed.

A good example of a comprehensive approach to OS security is the recently published Android Security Model ([the second version was released in December 2020](#)). System security is guided by the threat model. Each component of security is chosen intentionally and helps to mitigate a certain threat.

At the same time, 2020 proved that OS security still has a long way to go. Google Project Zero [published an analysis of a complex malware system](#) that used a chain of zero-day vulnerabilities. Serious malware is a high-quality product that has a modular architecture, command and control, and swappable components with exploits. As defenders, we should never underestimate attackers. Developing effective security tools requires that we look at OS security from an attacker's viewpoint.



**Mark Ermolov**

Lead OS and Hardware  
Security Researcher at  
Positive Technologies

## Hardware vulnerabilities

In 2020 we saw a softening of activity in information security and especially hardware security. I reckon this is because all the conferences went online and the number of participants declined sharply. However, it's not as if security experts stopped studying hardware vulnerabilities. If anything, right now is the lull before the storm. Researchers tend to keep their discoveries quiet, in order to make a show of them at upcoming conferences. In 2020, researchers were finally able to do pure research without having to spend time making slide decks or otherwise preparing for talks. The curtain will be sure to lift soon.

So we should expect to see a surge of hardware vulnerabilities. A recent major leak of confidential data related to Intel platforms (Exconfidential



Lake) has spurred interest. It was certainly a unique event: the public gained access to software emulators for new Intel platforms that were not yet on the market, which allowed researchers to look for vulnerabilities in firmware without even having to purchase the real thing. Researchers gained a head start by having the opportunity to study hardware long before release. This means that 2021 will likely bring plenty of discoveries of vulnerabilities in Intel firmware and hardware. Of course, the legality of using the leaked information is a separate issue. Researchers will hardly advertise the use of illegally obtained data or mention this in their articles. However, the bottom line is that researchers have become able to analyze many of the inner workings of Intel products for the first time. This leak is a vivid example of why security through obscurity does not work. I'm sure that soon we will reap the sad rewards of decisions made at some point by industry leaders. Unfixable hardware vulnerabilities and architecture flaws that can only be addressed in new products will hurt end users and, ultimately, vendor credibility.



**Nikolay Anisenya**

Head of Mobile Application  
Security at Positive  
Technologies

## Mobile security

In 2020 the world slowed down just a bit, which affected even the virtual world of IT, and especially mobile applications. We had to learn to live in a new way. In spite of that, some exciting developments happened in mobile security.

The slogan of last spring was "Stay home." This was the message from leaders in most countries. Business also had to adjust and shift to being at home wherever possible. Remote work has raised questions of supervision, communication, and security. There are 10 billion personal mobile devices in the world, with two thirds of users combining personal enjoyment with work on their devices ([techjury.net/blog/byod](https://techjury.net/blog/byod)). Clearly, many people use more than one device for work, and in most cases the second device is a smartphone. And now, with working from home becoming the new standard, these numbers have only increased.

Desktop operating systems make it easier for system administrators to protect desktop PCs and laptops: security software can be run with superuser privileges, while employees use accounts with only the privileges needed to do their jobs. But mobile devices are a different story. Popular mobile operating systems do not support privileged processes, leaving system administrators to rely on OS tools for mobile device management (MDM).

## Privacy protection

There is also the question of privacy. Whether your smartphone belongs to you or your employer is not so important. In either case, you can still install non-work apps. Users have an average of 67 apps on their phones, which raises security concerns.

With iOS 14, Apple introduced a number of important features intended to protect user privacy. For instance, app permissions now distinguish precise location from approximate location. Users can select which one they want to share with apps. Also, if an app wants to track users, it must explicitly ask

for permission. And finally, a new banner alert informs when an application is pasting from the clipboard (and therefore can read data you copied). In the first days after the release of iOS 14, dozens of popular applications were accused of [spying on users](#). Given that people tend to use their smartphones for remote work, such incidents may become a serious threat to corporate security. On the part of Apple, it was a major step towards increasing app transparency.

However, privacy should concern both business and ordinary cyberdenizens. Google and Apple, the two major mobile OS developers, meant well when creating the [Exposure Notifications System](#)—an API used to trace contacts with people infected by the coronavirus. It has long been available in the latest versions of Android and iOS. However, like any technology, the Exposure Notification API can also be used in harmful ways: instead of tracing those who have been infected, the API can allow potential attackers to [create a map of the user's movements](#). This is a good example of how new solutions can cause new problems, new questions, and—for security experts—new challenges.

Incidentally, these concerns do not apply to the owners of Huawei devices, which do not have this API. In 2020, Huawei moved from words to action as it started to abandon Google services and shift to the company's self-developed HarmonyOS 2.0 operating system. The first HarmonyOS 2.0 smartphones are expected to hit the market this year. It looks like the two mobile OS giants will have to make room for a newcomer. As for us, meanwhile, we will continue monitoring industry changes and contributing to the security of mobile apps.



**Alexandra Murzina**

Lead Advanced Technologies  
Specialist, Application Security  
Research, Positive Technologies

## Security and AI

Machine learning in information security long ago stopped being "rocket science." It has matured nicely with certain methods and solutions for approaching typical tasks. There are both advantages and pitfalls of using AI for analysis, quick response, and protection. The best option is to combine traditional techniques with the latest inventions.

According to the [Capgemini Research Institute](#), nearly two thirds of companies surveyed in 2019 think that AI will help to identify critical threats. And 69 percent believe that AI will be essential for quickly responding to cyberattacks. In 2019, only one in five organizations used AI. However, in 2020, this figure increased to almost two out of three.

AI has huge potential for strengthening cybersecurity. It can analyze user behavior, deduce patterns, and spot anomalies. Network vulnerabilities can be spotted quickly. AI can also help to automate routine security operations, letting teams focus on tasks requiring more human involvement and judgment. Companies can use AI to speed up malware detection.

AI is being increasingly used in areas outside IT. AI techniques, especially machine learning, require large amounts of data. Big data can help to improve products, but it can also be used to analyze user behavior for profit.

Finding and hiring a security expert or data scientist is already hard enough. The number of pros who know both fields is smaller still. Security is getting more and more difficult, because developers either do not know about the possible risks or prefer to put off dealing with them until only after a

product is released. The consequences can be dangerous. In Q1 2020 alone, large-scale data breaches increased by 273 percent.

At the same time, AI itself is code that can be vulnerable and create risks. In fall 2020, MITRE and Microsoft released a threat matrix for machine learning systems. In addition to Microsoft, 16 research groups took part in the project. The risks, having been verified on machine learning (ML) systems, are more than just theoretical. The resulting matrix resembles the ATT&CK matrix already familiar to researchers. Some of the risks are ML-specific. Others are characteristic of software in general but, because of residing in the software projects in which ML is used, may affect it indirectly.

Speaking about AI as a tool for attacks, it is important to mention deep-fakes incorporating powerful face- and voice-swapping techniques. Making convincing fakes is no longer difficult. There are many examples and trained machine learning models available on the Internet. App stores offer a variety of programs that allow ordinary users to swap faces and achieve very realistic results. In 2019, criminals used AI-based software to steal €220,000. In 2021, fraudsters made easy money by copying the face of neuroscience popularizer and Dbrain founder Dmitry Matskevich for a deepfaked announcement inviting users to join a blockchain platform.

On the one hand, the few AI security incidents to date hardly merit an all-hands-on-deck response. On the other hand, cases involving major companies (including Google, Amazon, and Tesla) have become a wake-up call for researchers and the whole IT industry to take the issue seriously. Overall we see a trend toward improved awareness regarding AI security, as well as development and implementation of better approaches.

---

## About Positive Technologies

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

For 19 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media ([LinkedIn](#), [Twitter](#)) and the [News](#) section at [ptsecurity.com](#).