Russia’s invasion of Ukraine has permanently altered the cyberthreat landscape. Leading up to the invasion, there is evidence that Russian hackers targeted a number of Ukrainian systems, and in years past, many suspect they conducted attacks on Ukrainian critical infrastructure and banking systems. In 2021, the US formally accused Russia’s spy agency of carrying out the SolarWinds hack to infiltrate US and European government networks. Today, government cybersecurity agencies around the world are warning of increased cyberattacks and espionage. In this report, we detail why and how every organization must prepare for a new era of cyberthreats.
Your brand’s corporate stance and actions make you a target. Dozens of companies from Apple to Netflix to Visa and Mastercard have stopped services and operations in Russia. Energy giants BP, Exxon, and Shell are walking away from Russian investments and partnerships worth billions. Iconic brands such as Coca-Cola, McDonald’s, and Starbucks suspended operations in Russia as a symbolic gesture after mounting public pressure and criticism that operations contradict the brands’ values. Whether your organization is taking direct economic steps or merely using words such as “war” and “invasion” in your public communication of support — words that contradict Russia’s narrative — this makes you a target for cyber retaliation or cyberespionage today and long into the future.

You will have to defend against several types of adversaries. Not all attacks will be Russian-state sponsored; they can be affiliated actors, or even permitted actors. These malicious actors may have similar political and ideological motivations, but their goals and tactics, techniques, and procedures (TTPs) may differ. On March 7, 2022, the US Department of Treasury advised financial institutions to increase vigilance for Russian attempts to evade sanctions via cryptocurrency. State-permitted cybercriminal syndicates such as Conti, and other ransomware-as-a-service operators sympathetic to Russia, will want to cause short-term disruption and raise funds for themselves and other causes. Be ready for all types.

Revenge, ideology, and outside influence will increase malicious insiders. These are powerful motivators for insider threats. In North America and Europe, there is widespread condemnation of Russia’s actions. However, it would be a mistake to assume this sentiment is universal. As companies continue to show support for Ukraine or take significant measures to cut ties with Russia, not all employees will
agree ideologically or politically with these moves, and some may have deep concerns about colleagues, friends, and family affected by these actions. In addition to the retailers closing operations in Russia, several of the major accounting firms and consultancies, including Deloitte, EY, KPMG, and PwC, have announced they will exit Russia, which will affect thousands of employees.

- **Cyberoperations is a permanent feature of the landscape.** Everyone wants a quick and peaceful solution to Russia’s invasion. Let’s all hope for one. However this conflict unfolds and resolves, the use of cyberoperations as a precursor to military conflict, a tactic of military operations, and tool of retaliation is here to stay. In all future military conflicts, great and small, expect both sides to spread and amplify disinformation, soften targets with preemptive cyberattacks on government and critical infrastructure, sow chaos and fear with cyberattacks on allies and supporters, raise funds through ransomware, and steal intelligence and competitive IP with cyberespionage. This is our new reality.

**Take Control Of Communication To Your Teams And Your Executives**

Cybersecurity incidents that achieve media prominence have a habit of alarming senior executives and board members, resulting in a cascade of panicked questions to you and your team. Don’t be caught unawares, as such requests can consume precious time that you will need to deal with a potential incident. To avoid drowning in a deluge of panic and requests:

- **Relentlessly and proactively update your executives.** Prepare a brief in advance and make it factual to avoid further fear. Include your external threat reporting, but enrich it with internal context, highlighting the potential impact on your organization and the overall risk to the business. Take the opportunity to remind your executives what tactical activities you’re undertaking to deal with the immediate issues, as well as how your strategy will serve to prepare for such events, now and in the future. Be clear on when you will update the executives next, and what topics you’ll cover. Reassure them that if there is a major incident, you’ll update them per the major incident processes of the organization.

- **Develop a “Ukraine/Russia War FAQ” document for your board and executives.** In many organizations and regions, security is a new and scary topic for execs and board directors. Make their lives easier by creating reference materials such as an FAQ to guide discussions. This will help execs ask the right questions about the implications of the war, such as “What is the current advice from our government?” or “What is our current level of risk?” Not only will you get the opportunity to guide the discussion, but you will invite an open line of communication with your stakeholders and give them the opportunity to engage with you in a meaningful
and safe way.

• **Be ready for more misinformation and disinformation.** Misinformation and disinformation featured heavily in the lead-up to this conflict. Allegations of staged cabinet meetings well after decisions were made are one example. On February 3, the US predicted Russia would use graphic fake videos as pretext for invasion. Open source intelligence researchers analyzed a video that surfaced two weeks later proving the US correct. In France, India, the UK, and the US, respondents to our March 2021 Global Trust Imperative Survey said they trusted their employers more than their national and local government leaders. This means the information your security team provides carries considerable weight. So, keep your incident response plans and their communication elements handy.

• **Consider secure communications tools for security, privacy, and reliability.** Firms concerned about the security and privacy of business communications — such as eavesdropping, communications metadata exposure, data loss, or noncompliance — should take steps to protect corporate communications. While consumer apps like WhatsApp and Telegram are popular and free, take this opportunity to educate executives about the risks when employees use them for business purposes. Employees in and around Ukraine may also face disruptions to communications infrastructure. Enterprise-class encrypted messaging and calling solutions like Element, KoolSpan, and Wickr work in low-bandwidth environments. And these tools aren’t one-off investments; you can use them to protect everyday communications, as out-of-band communications channels during incident responses, and to provide traveling executives with enhanced security.

**Build A Closer Relationship With Government Agencies And Your Strategic Vendors**

Security leaders will find an invaluable ally in government agencies. These agencies have come a long way from the Orange Book days and the government types who thought security would be easy if only the internet was shut down. In the US, the Cybersecurity and Infrastructure Security Agency (CISA) has added significant value to both the US and global debate in emergency security incident response situations, issuing high-quality and practical advisories on everything from SolarWinds to Log4j. In the UK, the formation of the National Cyber Security Centre (NCSC) marked a clearing out of the old guard, and like its US counterpart, has won plaudits for the practicality of its advice for private sector organizations. The EU as well has upped its game, with cross-regional threat intelligence sharing and computer emergency response team (CERT) support for Ukraine just some of the assistance its agencies have provided. To take advantage of this support:
• **Follow current advice from your national cybersecurity authority.** Through its Shields Up initiative, CISA has warned of increased attacks on critical infrastructure and defense industrial bases. This is the best place to receive up-to-date information on the current state of the conflict. In the UK, the NCSC has also published specific steps to take. Other agencies, including the European Union Agency for Cybersecurity (ENISA), the Federal Office for Information Security (BSI) in Germany, and the National Cybersecurity Agency (ANSSI) in France, have warned of the situation. The Australian Cyber Security Centre also provided guidance when it placed sanctions on Russia on February 23. In the absence of specific information from your national cybersecurity authority, use the guidance we’ve linked [here](#).

• **Reach out to government contacts.** Make sure you have a stable contact within the government in each country where you have a large operation so you can reach out in case of an incident or for updates on the current situation. In the United States, InfraGard coordinates information sharing with critical infrastructure providers. In the UK, review information provided by the UK NCSC Critical National Infrastructure hub and its equivalents in Europe. For EU-based organizations, speak to your local computer security incident response team (CSIRT) and CERT contacts. ([Find a full listing here.](#))

• **Demand more from your strategic security vendors.** Your security vendors must take a proactive role in your preparations for cyberconflict. Rely on your account representatives; they’re incentivized to ensure you receive the proper level of care contractually or specific to that technology. For product vendors, confirm turnaround time and automation options for ruleset and patch updates; for managed services, clarify their processes and communication channels. Vendors should already be sending you communications about the conflict. If you have yet to receive updates, reach out directly. Pay particular attention to vendors that were less responsive during Log4Shell, because two subpar performances during a crisis is an alarming pattern.

### Develop Better Intelligence And Make It Actionable

The world’s intelligence agencies have done a remarkable job of coming together and sharing intelligence to limit misinformation and disinformation. They have the information you don’t have. CISOs must focus on preparation and on improving your firm’s resilience rather than trying to predict how the conflict will continue to unfold and how this will alter the cyberoperations and cyberattacks of state-sponsored, affiliated, and permitted cyberadversaries. We recommend that CISOs:
• Create a list of trusted sources of geopolitical and cyberthreat intelligence (CTI). During the pandemic, heads of HR and response teams created curated lists of government agencies, academic institutions, and consultancies for intelligence and recommended responses. Do the same here, focusing on noted international relations and CTI experts and ignoring everyone else. Aside from CISA and the US Department of State (or regional equivalent), look at think tanks like the Belfer Center and the Council on Foreign Relations. When sharing information and predictions with the executive team, refer to one or more of your trusted sources. Share your list with your team, and encourage them to look to these experts for guidance when they're tempted to react to the latest rumor.

• Initiate a “request for intelligence” from your CTI vendor. Ideally, this is an existing part of your contract — but it’ll be worth it even if you must pay an additional fee. Explain the target audience for the report so that your vendor will produce information at the right altitude (for your board of directors, for your security team, etc.). The request for intelligence should go beyond the normal overviews your vendor provides, and it should include specifics related to your vertical industry and operating locations. Further, it should give you information on threat actors of concern and on the TTPs that those threat actors use.

• Operationalize intelligence. CISOs continue to seek higher-fidelity intelligence to better meet organizational requirements, which often leads to subscribing to more commercial and open-source intel feeds. Increasing feeds and data sources doesn’t guarantee more accurate or complete CTI. With a potential surge in new intel relating to the current conflict, CISOs should resist the urge to bring on new intel sources before first determining if it’s accurate, complete, relevant, and timely. If it meets those requirements, then you can consider subscribing to it, while keeping an eye on the costs and time required to operationalize it. If you can’t operationalize the intel fast enough (e.g., not until after the cyberattack has begun), its value is diminished.

• Focus threat hunting efforts on related, trusted intelligence. Security teams should build their own personal threat model for the current conflict and direct their threat hunters to use it as a starting point for hunts. Now is the time to focus threat hunting efforts on trusted intelligence sources related to the conflict as an assurance exercise. Further, if there is downtime for security analysts to start threat hunting, encourage them to research new intel related to the conflict and hunt for attacks based on that data.

Bolster Your Essential Security Defenses — Especially Vulnerability And Patch Management
It’s too late to initiate widespread technology changes to protect against the attacks that are likely to occur in the next few weeks and months. However, there are services that are quick to deploy and that can protect public- and client-facing applications and websites. You can also ensure you’re at least doing the basics right, and if there are adjustments you can make after a recent tabletop session to processes or communication, make them — and update your documentation accordingly.

- **Revisit your DDoS protection.** The internet is far too large and open to prevent actors from orchestrating DDoS attacks against the Ukrainian allies and supports from agents provocateurs all over the globe; in fact, this has already happened. The February DDoS attacks against a Ukrainian bank were coordinated by a C2 server hosted in the Netherlands, using the VegaSec botnet, the source code for which is available on GitHub. For this reason, you can’t assume a cyber-isolated Russia will ensure your own safety; nor will geoblocking Russian netblocks. Adding urgency to the situation: Since mid-February, attackers have been using a new DDoS amplification technique (CVE-2022-26143) with the largest magnification factor ever recorded (in the billions).

  Take three steps immediately: 1) ensure that you have agreements with one or more DDoS providers; 2) audit your web properties to ensure that they either have DDoS protection or that it can be marshalled quickly in the event of a direct attack or collateral damage; and 3) review your incident response plan to ensure it includes procedures and contact information in case of a DDoS attack.

- **Take the simple steps to start your Zero Trust journey.** Zero Trust is not just a model, it’s also a journey. Zero Trust provides a roadmap for long-term protection against attacks. Look for the most readily addressed issues in your environments for the short term, specifically, privileged accounts, as they hold the keys to the kingdom and, if compromised, can be an organization’s downfall. This step alone can significantly reduce the impact of a privilege escalation attack without requiring a heavy lift for the SOC team. Use Forrester’s Practical Guide To A Zero Trust Implementation to identify areas where you’ll get the most benefit the fastest. Security leaders should use this crisis to strengthen your organizational defense as you prepare to move further down the path toward a robust Zero Trust implementation.

- **Pay attention to device and software hygiene.** This is a critical time to get your devices, endpoints, and applications fully patched and up-to-date. Forrester’s 2021 data shows that software vulnerability exploits are the most common vector for external attacks. Subscribe to the CISA Known Exploited Vulnerabilities Catalog Update Bulletin. Prioritize critical vulnerabilities and any vulnerabilities with a known exploit, but don’t neglect highs and mediums; an unrelated attacker who
has been hoarding a backlog of exploits might well decide to use them while the world is preoccupied with the war in Ukraine. In addition, consider a tabletop exercise around responding to and patching a new zero-day.

**Deter attacks that adversaries use to fund other criminal activities.** Teams often write off attacks like ad fraud as the cost of doing business, but such attacks are highly profitable and feed criminal syndicates. Last year’s sentencing of Aleksandr Zhubov — who engineered a massive ad fraud campaign from Russia and Bulgaria, ultimately stealing over $7 million — reminds us that ignoring such activities could directly or indirectly support both physical and cyberattacks against our nations and organizations. Shore up your protections against ad fraud and other automated attacks with a solid bot management solution, and work across your business to understand these hidden attacks that could be profiting adversaries.

**Prioritize insider risk.** Insiders (employees, contractors, vendors, partners) may be motivated to turn malicious. To protect against this, cut off access for any departing users, especially those left behind in Russia. Monitor users who may sympathize with Russia or those affected by shutdowns for signs that they could use their access to sabotage data or systems or could share sensitive information externally. Have a plan to render useless any devices and data departing users may still retain. Russian operatives may also be reaching out to users to convince them to share authentication credentials or plant malware in your systems. Beef up monitoring of users, especially those at higher risk.

**Invest In The Breadth And Depth Of Your Incident Response Capabilities**

For the past two years, all eyes have been on ransomware attacks — as were all incident response (IR) plans and tabletop exercises. While ransomware remains a threat requiring continued vigilance, firms must also review and refine IR plans and develop crisis simulations to reflect the increased threat of a targeted attack. Designed and executed for maximum gain, be it the destruction of critical infrastructure or the delivery of valuable information, targeted attacks and the attackers behind them won’t announce themselves, and they aren’t looking for the easiest way in. Now is the time for security leaders to engage executives in frank discussions about the risk and impact of a targeted attack and the resources needed to respond. From there, leaders must:

**Create and run simulations for targeted attacks and vary them by region.**

Engage immediately with your cybersecurity IR service provider — or select and retain one with expertise beyond ransomware response — to review your IR plan and targeted attack-specific playbook. Use your provider’s experience in responding to and investigating attacks attributed to nation-states to develop
realistic targeted attack simulations. Not only should you run these exercises at the technical and executive level, but you should tailor and perform them in each geographic region in which the firm operates. Document and incorporate your findings from simulations into the IR plan and region-specific playbooks and repeat them within a few weeks to ensure you perfect processes and teams are prepared.

- **Ruthlessly prioritize your incident responders’ workloads.** Incident responders and seasoned team members will be doing the heavy lifting in the event of nation-state and high-priority attacks. To avoid burnout of these critical personnel, rely on lower-level security analysts to streamline triaging, prioritization, and resolution of most incoming attacks. According to Forrester’s Business Technographics Security Survey, analysis takes the longest of any aspect of the IR process — so where possible, use security analysts to do the heavy lifting for the IR team. Selectively use your incident responders for response to highly sensitive high-risk, high-impact attacks.

- **Build your incident responder ranks.** If you’ve been looking to create a path for advancement for your high-performing SOC analysts or security engineers, now is the time. Many IR service providers offer training for internal teams on response actions, forensic investigations, and evidence collection. A targeted attack usually results in a complex, protracted response. Work with your provider to develop a training plan that creates a bench of capable understudies on the promotion path so that you can allow your key responders to rest.

### Understand The Implications Of Laws Governing Data And Service Provider Obligations

A war is not the time to dwell on legal subtleties. However, if you’re making decisions on how to manage data during this crisis, you must get familiar with the implications of some legal concepts. Critical concepts include: data residency (a requirement to store and/or process data in a certain region), sovereignty (the “rules of the land” governing the data); localization (a requirement to always keep local copies of the data in the country where data is collected), and the legal obligations that services providers managing your data must meet. We recommend that CISOs and chief privacy officers:

- **Develop a plan for localization of Russian PII before you exit your Russian operations.** If you have collected the personal data of Russian citizens, you must maintain a copy of it on servers within Russian borders. This requirement is in place to ensure the government has access to the data at any time. This only applies to PII, hence you don’t need to leave copies of other data as you move out. As you plan your migration strategy, ensure you understand the rules and
regulations of the region to where you will move your data.

• **Prepare for a bevy of government requests to access PII.** Don’t assume storing and/or processing data in a certain region provides de facto protection from foreign access. Regardless of where you store data, governments can still ask services providers under their sovereignty to provide access at any time. For example, the US government can request access from US-headquartered cloud companies even for data they store in European data centers. And, under the threat of a global war, public health and safety will become an easy way for every government to gain access; GDPR and other privacy regulations always include exception policies for national security, safety, etc. Ensure you know which governance and technical measures your cloud provider has in place to manage governments’ access requests. If you manage your own encryption keys, ensure you have extra capacity in case your assistance is required.

• **Don’t underestimate the risk of attacks on services providers.** Services providers are companies that act under the jurisdiction of their governments. Hence, they can become targets by themselves or by association to their national governments. Your data might be in danger even if you keep it in the most regulated country. This means that, for example, an attack on a US services provider that manages your data might have a significant impact on your assets even if they’re stored far away.

• **Ensure that your migration strategy is not the weakest link.** To increase your organization’s resilience and security, you might be planning to migrate data from one region to another. Experience has taught us that transferring data can create vulnerabilities that can be easily exploited. Ensure you encrypt your data in transit, choose robust encryption key management policies, and apply extra identity and access controls for the duration.

**Supplemental Material**

**Research Methodologies**

Forrester’s March 2021 Global Trust Imperative Survey was fielded globally to 1,851 online adult respondents. Forrester fielded the survey in March 2021. Respondent incentives included a summary of the survey results. Exact sample sizes are provided in this report on a question-by-question basis.

This survey used a self-selected group of respondents and is therefore not random. This data is not guaranteed to be representative of the population, and, unless otherwise noted, statistical data is intended to be used for descriptive and not
inferential purposes. While nonrandom, the survey is still a valuable tool for understanding where users are today and where the industry is headed.

Forrester’s Consumer Energy Index Survey, US Consumers, May 2020, was fielded in May 2020. This online survey included 500 online adults (18+) in the US. Forrester leveraged Dynata to recruit respondents and conduct the survey research.
We help business and technology leaders use customer obsession to accelerate growth.

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We’re on your side and by your side to help you become more customer obsessed.

Research
Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting
Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events
Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2022 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.