The Resilience Issue
How your business can adapt and thrive in times of crisis
Contents

2 EDITOR’S LETTER
COVID-19 reminded us why business resilience matters
by Gina Mastantuono

4 BUSINESS TOUGHENS UP
A new global survey shows which types of organizations are making headway with resilience—and how

6 A YEAR LIKE NO OTHER
Resilient leaders doubled down on digital transformation and thrived during the pandemic

7 KEEPING THE SHELVES STOCKED
Digital solutions for snarled supply chains
by Thomas Lee

TECHNICALLY SPEAKING
Risk management jargon can be impenetrable. Don’t worry, Workflow has you covered

8 A NEW ERA OF OPERATIONAL RISK
Risk managers will face new challenges after the pandemic abates
by Christopher Null

14 THE COVID DIVIDEND
ServiceNow’s Bob Osborn explains how pandemic-fueled investment is transforming public sector IT

18 ORGANIZATIONS NEED ‘PRIVACY BY DESIGN’
In today’s world, privacy safeguards must be baked into every process, product, and service to meet evolving cyberthreats
by Evan Ramziopoulou

22 “IKIGAI” IS THE FUTURE OF WORK
How an ancient Japanese philosophy could help create healthier, more connected workplaces
by Christina Lee

25 CONTRIBUTORS
Welcome to the Resilience issue

Companies need resilience to succeed in a world where disruption occurs suddenly and cascades unpredictably.

“...A good half of the art of living is resilience,” writes contemporary philosopher Alain de Botton. The same is true for the art of building a successful organization.

We define organizational resilience as the ability to maintain performance in the face of environmental, political, social, cyber, and other disruptions. The global pandemic reminded us that in an interconnected world, disruption can occur suddenly and cascade unpredictably.

At the same time, some companies and governments weathered the COVID-19 challenge better than others. So what are the attributes that distinguish the world’s most resilient organizations? How should leaders orchestrate people, processes, and technology to take resilience—and its twin, risk management—to the next level of excellence?

To help answer these questions, we worked with ESI ThoughtLab to survey more than 1,080 senior business leaders across six industries in 13 countries around the globe. Company sizes ranged from $350 million to more than $5 billion in annual revenue.

We ranked our respondents as leaders, intermediates, or beginners based on the progress they reported in key resilience areas, such as modernizing tools for planning and response, building a resilience-focused culture, digitizing workflows across the enterprise, and introducing cross-functional risk management.

Our results highlight the practices that distinguish resilience leaders from laggards, along with the performance gains that accrue from moving up the resilience curve.

Enterprises face a mix of organizational and technical challenges to building resilience. The top one is uncertain ROI and business case—an obstacle that can prevent some from putting in place the technologies and processes they need. Organizational silos further complicate resilience efforts.

For beginners, resilience is a relatively new concept. Since much of it is about prevention and preparation, as well as about recovery, beginners often find it difficult to demonstrate a business case and ROI. Beginners also struggle more with lack of skills and know-how.

As organizations advance, these issues become less of an impediment. Instead, intermediate-stage organizations are burdened with organizational obstacles, such as siloed data and varying mentalities across teams.

Leaders face different challenges around systems and data. Leaders see much larger roadblocks from systems requiring too much configuration, lack of budget for more advanced techniques, difficulty in modernizing processes, and outdated or inaccurate data.

Leaders and laggards also diverge in the benefits gained from various resiliency steps. For example, nearly twice as many leaders report improved customer satisfaction and higher shareholder value as benefits, compared to laggards. Leaders also enjoy more profitability, higher staff productivity and retention, as well as greater market share.

The performance boost that leaders gain from their efforts argues for a much more proactive approach to building resilience by all organizations. While we can’t predict future challenges, we can strive to make our organizations ready for whatever comes. That’s why we packed this issue of Workflow Quarterly with insights and recommendations to help you build resilience into every corner of your company.
Business toughens up

Every organization today is striving to become more resilient. A new global survey shows which types are making headway, and how.

Resilience progress by region

Percentage of organizations ranked as resilience leaders

- **U.S.**: 26%
- **Europe**: 15%
- **Asia/Pacific**: 21%

**Resilience progress by sector**

Percentage of resilience leaders in 5 major industries

- **Financial Services**: 26%
- **Healthcare**: 19%
- **Telecom**: 17%
- **Manufacturing**: 18%
- **Public Sector**: 11%

**Most effective resilience strategies by industry**

- **Financial Services**: Nimble supply chains
- **Healthcare**: ESG risk management
- **Manufacturing**: Resilience audits
- **Public Sector**: Resilience reporting tools
- **Telecom**: Third-party risk management

Source: ServiceNow/ESI ThoughtLab survey of senior business leaders across six industries in 13 countries worldwide.
A year like no other
Resilient leaders doubled down on digital transformation and thrived during the pandemic

Digital Maturity Index scores rose sharply across industries worldwide

ServiceNow’s Digital Maturity Index is a patent-pending algorithm that measures the digital maturity of more than 7,000 companies and government agencies that host operational data on the Now Platform. The DMI provides unique visibility into how intelligent workflows powered by AI and machine learning are changing how companies operate and go to market. DMI data from 2020 shows that many companies responded to the pandemic by accelerating their digital transformation to weather the storm.

- During the COVID-19 pandemic, DMI scores rose sharply across industries worldwide. DMI scores rose 14.3% in government, 12.5% in retail and wholesale, 10.9% in healthcare and life sciences, and 8% in financial services.
- Driven by pandemic-fueled surges in work from home, distance learning, and online shopping, digital workloads on the Now Platform skyrocketed by 26.1% in 2020.
- Automation levels rose 14.3%, as increased workloads forced companies to automate at scale. At the same time, health and safety concerns fueled the rapid development of custom apps on the Now Platform.
- The education sector saw a 20.1% DMI rise, fueled by digitally enabled distance learning.
- Manufacturing and natural resources saw a 15.5% DMI increase, driven by increases in digital workloads and automation.

The maximum risk an organization is willing to take for each type of risk

Operational resilience
An organization’s ability to anticipate, prevent, respond, recover, and adapt to operational disruptions. The term can be applied to areas such as technology, facilities, people, and third-parties.

Operational risk
The risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events.

Risk appetite
The amount and type of risk that an organization is prepared to pursue, retain, or take.

Risk tolerance
The maximum risk an organization is willing to take for each type of risk.

Security information and event management (SIEM) system
Software that allows computer security professionals to analyze real-time data from across an entire enterprise IT network to detect, deflect, and prevent cyberattacks.

Shadow IT
IT services used by company employees outside the control or knowledge of corporate IT departments.

ServiceNow’s Digital Maturity Index is a weighted composite index based on: user reach, as measured by active ServiceNow users as a % of the total employee base; workload, derived from incidents, requests, knowledge views, HR and CSM cases; and automation, measured by the extent a company uses digital workflows, orchestration, knowledge views, HR and CSM cases; and automation, measured by active ServiceNow users as a % of the total employee base.

Keeping the shelves stocked
The pandemic exposed cracks in digitally enabled global supply chains

BY THOMAS LEE

As the global pandemic hit full stride last year, consumers looking for toilet paper and soap discovered empty shelves. The global supply chain buckled. Although manufacturers eventually recovered, the prospect of future shortages looms. Retail industry consultant Carol Spicerman says that manufacturers and retailers, who normally spar over pricing, must work together to ensure goods get to consumers throughout the crisis.

Why did we see product shortages at the start of the pandemic?
The reason for the shortages has to do with technological developments in inventory management. Companies run lean operations and only order goods when they really need them. But when you have erratic buying and a surge in demand, it throws all of those algorithms and models out the window. The lack of precedent is another problem because generally models are built on past behavior and historical data. And once you’re behind, it’s really hard to catch up.

Is it possible to “pandemic proof” the supply chain?
It’s really difficult to come up with universal solutions because there are so many moving parts in the supply chain. But, everybody has to have really clear communication going forward. Talking to my clients, I have definitely seen a lot more transparency and a lot less shenanigans in terms of trying to hide the truth or pretty things up when products aren’t going to be delivered or when they’re going to be just outright canceled. The manufacturers and wholesalers who are transparent and honest are going to come out better on the other end of this.

Can domestic manufacturing companies step up and fill gaps in the supply chain?
I’ve spoken with companies that are relying much more heavily on U.S. manufacturers. In the past, companies said it was too expensive to make things in America. But now overseas shipping costs are prohibitively expensive. It’s getting so bad you can make a case that it makes more economic sense to manufacture things domestically. But you can’t turn up a manufacturing capability on a dime. You can say that U.S. manufacturing is certainly part of the solution, but there’s no way it can be a total solution.

Jargon helps insiders message tribal affiliation, but can seem impenetrable from the outside. Here’s a cheat sheet to key terms in the field of risk management and resilience.

Risk appetite
The amount and type of risk that an organization is prepared to pursue, retain, or take.

Risk tolerance
The maximum risk an organization is willing to take for each type of risk.

Operational risk
The risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events.

Operational resilience
An organization’s ability to anticipate, prevent, respond, recover, and adapt to operational disruptions. The term can be applied to areas such as technology, facilities, people, and third-parties.

Security information and event management (SIEM) system
Software that allows computer security professionals to analyze real-time data from across an entire enterprise IT network to detect, deflect, and prevent cyberattacks.

Shadow IT
IT services used by company employees outside the control or knowledge of corporate IT departments.

Why did we see product shortages at the start of the pandemic?
The reason for the shortages has to do with technological developments in inventory management. Companies run lean operations and only order goods when they really need them. But when you have erratic buying and a surge in demand, it throws all of those algorithms and models out the window. The lack of precedent is another problem because generally models are built on past behavior and historical data. And once you’re behind, it’s really hard to catch up.

Is it possible to “pandemic proof” the supply chain?
It’s really difficult to come up with universal solutions because there are so many moving parts in the supply chain. But, everybody has to have really clear communication going forward. Talking to my clients, I have definitely seen a lot more transparency and a lot less shenanigans in terms of trying to hide the truth or pretty things up when products aren’t going to be delivered or when they’re going to be just outright canceled. The manufacturers and wholesalers who are transparent and honest are going to come out better on the other end of this.

Can domestic manufacturing companies step up and fill gaps in the supply chain?
I’ve spoken with companies that are relying much more heavily on U.S. manufacturers. In the past, companies said it was too expensive to make things in America. But now overseas shipping costs are prohibitively expensive. It’s getting so bad you can make a case that it makes more economic sense to manufacture things domestically. But you can’t turn up a manufacturing capability on a dime. You can say that U.S. manufacturing is certainly part of the solution, but there’s no way it can be a total solution.

Jargon helps insiders message tribal affiliation, but can seem impenetrable from the outside. Here’s a cheat sheet to key terms in the field of risk management and resilience.

Risk appetite
The amount and type of risk that an organization is prepared to pursue, retain, or take.

Risk tolerance
The maximum risk an organization is willing to take for each type of risk.

Operational risk
The risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events.

Operational resilience
An organization’s ability to anticipate, prevent, respond, recover, and adapt to operational disruptions. The term can be applied to areas such as technology, facilities, people, and third-parties.

Security information and event management (SIEM) system
Software that allows computer security professionals to analyze real-time data from across an entire enterprise IT network to detect, deflect, and prevent cyberattacks.

Shadow IT
IT services used by company employees outside the control or knowledge of corporate IT departments.

Why did we see product shortages at the start of the pandemic?
The reason for the shortages has to do with technological developments in inventory management. Companies run lean operations and only order goods when they really need them. But when you have erratic buying and a surge in demand, it throws all of those algorithms and models out the window. The lack of precedent is another problem because generally models are built on past behavior and historical data. And once you’re behind, it’s really hard to catch up.

Is it possible to “pandemic proof” the supply chain?
It’s really difficult to come up with universal solutions because there are so many moving parts in the supply chain. But, everybody has to have really clear communication going forward. Talking to my clients, I have definitely seen a lot more transparency and a lot less shenanigans in terms of trying to hide the truth or pretty things up when products aren’t going to be delivered or when they’re going to be just outright canceled. The manufacturers and wholesalers who are transparent and honest are going to come out better on the other end of this.

Can domestic manufacturing companies step up and fill gaps in the supply chain?
I’ve spoken with companies that are relying much more heavily on U.S. manufacturers. In the past, companies said it was too expensive to make things in America. But now overseas shipping costs are prohibitively expensive. It’s getting so bad you can make a case that it makes more economic sense to manufacture things domestically. But you can’t turn up a manufacturing capability on a dime. You can say that U.S. manufacturing is certainly part of the solution, but there’s no way it can be a total solution.

Jargon helps insiders message tribal affiliation, but can seem impenetrable from the outside. Here’s a cheat sheet to key terms in the field of risk management and resilience.

Risk appetite
The amount and type of risk that an organization is prepared to pursue, retain, or take.

Risk tolerance
The maximum risk an organization is willing to take for each type of risk.

Operational risk
The risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events.

Operational resilience
An organization’s ability to anticipate, prevent, respond, recover, and adapt to operational disruptions. The term can be applied to areas such as technology, facilities, people, and third-parties.

Security information and event management (SIEM) system
Software that allows computer security professionals to analyze real-time data from across an entire enterprise IT network to detect, deflect, and prevent cyberattacks.

Shadow IT
IT services used by company employees outside the control or knowledge of corporate IT departments.

Why did we see product shortages at the start of the pandemic?
The reason for the shortages has to do with technological developments in inventory management. Companies run lean operations and only order goods when they really need them. But when you have erratic buying and a surge in demand, it throws all of those algorithms and models out the window. The lack of precedent is another problem because generally models are built on past behavior and historical data. And once you’re behind, it’s really hard to catch up.

Is it possible to “pandemic proof” the supply chain?
It’s really difficult to come up with universal solutions because there are so many moving parts in the supply chain. But, everybody has to have really clear communication going forward. Talking to my clients, I have definitely seen a lot more transparency and a lot less shenanigans in terms of trying to hide the truth or pretty things up when products aren’t going to be delivered or when they’re going to be just outright canceled. The manufacturers and wholesalers who are transparent and honest are going to come out better on the other end of this.

Can domestic manufacturing companies step up and fill gaps in the supply chain?
I’ve spoken with companies that are relying much more heavily on U.S. manufacturers. In the past, companies said it was too expensive to make things in America. But now overseas shipping costs are prohibitively expensive. It’s getting so bad you can make a case that it makes more economic sense to manufacture things domestically. But you can’t turn up a manufacturing capability on a dime. You can say that U.S. manufacturing is certainly part of the solution, but there’s no way it can be a total solution.
A new era of operational risk

Risk managers will face new challenges coming out of the pandemic

BY CHRISTOPHER NULL
If the COVID-19 crisis was a rude awakening for many tech CEOs, it was doubly so for enterprise risk managers.

For years, they gained experience navigating different kinds of financial crises, from the dotcom bust of 2001 to the 2008 market crash and ensuing recession. But there were no actuarial or risk models to guide them through what the pandemic threw at them—an overnight jump into remote work, employee health challenges, a spike in cybersecurity attacks, supply chain slowdowns and stoppages. The experience exposed major non-financial risks that many companies never expected or planned for.

“It was one of the biggest disruptions most companies have ever faced, and it put a lot of corporate frameworks of risk to the test,” says Tom Campanile, a partner in Ernst & Young’s financial services advisory.

Now for the bad news: The pandemic was just the start, according to Campanile and other risk experts. Just a few months away from 2022, many businesses face another shift in the way they manage an increasingly important area of risk—operational risk. The dramatic jump in the number and severity of cyber attacks, particularly ransomware events, has sent companies scrambling for new types of security solutions. The emergence of long-term hybrid working models similarly demands new planning about risk related to human resources and IT management.

Other continuing plot twists of 2021—including the spread of the COVID-19 Delta variant—have kept the enterprise in a state of flux. When it comes to getting people back in the office, “many organizations are trying to achieve the equivalent of putting the horse back in the barn,” says Mark Nicholson, principal with Deloitte Risk & Financial Advisory, adding that risk management processes, such as incident management and fraud mitigation tactics, are under more stress than ever. “Additional controls are required, which are somewhat difficult to automate given the current circumstances.”

**New focus on operational risk**

Much of this is still new territory for many companies. Until last year, operational risks hadn’t been widely scrutinized and analyzed, but now they’re taking center stage. According to a 2021 study by Risk.net, IT disruption, data breaches, and resilience risk rank as the top three operational risks in the enterprise.

Managing operational risk more comprehensively is crucial heading into 2022, says Campanile. “Risk has typically been managed in silos, but connecting the dots across those risks is key and requires different disciplines, plans, and working on different time scales.”

While arguably ignored, operational risk models have been available for years. ISO 31000, for example, is a set of guidelines from the International Organization for Standardization that identifies a wide variety of corporate risk factors. COSO, another framework developed by the Committee of Sponsoring Organizations of the Treadway Commission, is designed to uncover and prevent business fraud. It also has significant accounting and auditing components.

But the pandemic has exposed additional weaknesses. “The industry is still figuring this out,” says Nicholson.

Many employees in the financial sector, for example, are required to work at the office, specifically for risk management reasons; fudging accounting numbers is harder to do under direct supervision, Nicholson says.

But how will companies keep tabs on accounts with workers in hybrid environments? Some solutions simply increase other risk factors. Employee-monitoring systems can compromise privacy. Data stored on consumer devices invites security risks.

**Avoiding risk traps**

While most companies have processes for managing compliance and IT risks, such as service outages, many lack frameworks for handling larger yet more unforeseen threats. “They often end up focusing on high-likelihood but low-impact risk at the expense of anticipating and mitigating high-impact operational risk, such as the emergence of COVID-19,” says Barbara Kay, senior director of product marketing for security and risk at ServiceNow.

Executives must assess new risks as they navigate ongoing pandemic challenges. For instance, does working from home long-term—which reduces workplace safety risks—increase compliance and control risks?

“Take a step back and focus on the experience gained and lessons learned during this disruption,” says Campanile. “What worked and what didn’t? What assumptions in your response plans were underestimated or overestimated? Where did contingency plans or risk assessments fall short?”

A post-mortem assessment to identify opportunities for better alignment, he adds, “will be the foundation for revisiting the framework.”
**A new approach**

Digital enterprise risk management (ERM) systems can also be a helpful tool, allowing CFOs, CISOs, and others to centralize and consolidate risk management across different business functions. Tools such as desktop monitoring and configuration management, for example, "can help mitigate risk at the individual level, but what’s really needed is a high-level framework that focuses foremost on business resilience," Campanile says. "This is an opportunity for leadership to paint a firmwide picture of vulnerabilities."

The use of simulations can also help managers develop operational risk-assessment models. ERM platforms can conduct data-supported scenario analyses and live testing. "Tabletop" exercises, meanwhile, can involve a roundtable discussion about how to manage a hypothetical crisis. In Campanile’s words: "The intention is to play out a hypothetical scenario and use the output to strengthen existing capabilities."

The Dodd-Frank regulations, passed in the wake of the 2008 financial crisis, showed that new risk measures are usually imperfect, and managing risk is an increasingly complex discipline. "We’re at the intersection of data, identity, expectations of privacy, ethics, and more," Nicholson says. "It’s playing out at a rapid pace, but I don’t think we’ll see a resolution for up to a decade."

---

**TOP 10 OPERATIONAL RISKS 2021**

1. **IT disruption**
2. **Data compromise**
3. **Resilience risk**
4. **Theft and fraud**
5. **Third-party risk**
6. **Conduct risk**
7. **Regulatory risk**
8. **Organizational risk**
9. **Geopolitical risk**
10. **Employee wellbeing**

*SOURCE: RISK.NET STUDY ON THE TOP 10 OPERATIONAL RISKS FOR 2021*
The COVID dividend

ServiceNow’s Bob Osborn explains how pandemic-fueled investment is transforming public sector IT

The popular image of the public sector is the DMV: long waits, sclerotic bureaucracy, and ancient systems and processes that resist change or innovation. A recent ESI ThoughtLab and ServiceNow survey of more than 1,000 C-level executives would seem to support that stereotype. According to this research, the public sector is behind private companies when it comes to investing in resilience and risk management, even in the face of increased cyberattacks, ransomware, and other threats during the pandemic.

That, however, isn’t the whole story, according to Bob Osborn, ServiceNow’s chief technology officer of global governments. Osborn, who has held high-level federal IT jobs for the U.S. Army, U.S. Transportation Command, and the National Nuclear Security Administration, says that the pandemic has changed the public sector, perhaps for good.

ServiceNow’s recent Resilience survey found the public sector generally trails private companies in terms of resilience. Our respondents blamed this gap on rigid government systems and procedures. Does that seem right to you?

Osborn: In general, I would agree with that. There are agencies that have demonstrated maturity, resilient processes, and preparation from a technical standpoint to demonstrate resilience. Other agencies, not so much.

Most agencies rely on legacy technologies that require a great deal of manual intervention whenever there’s an issue, an outage, or an emergency. But there’s a caveat. Agencies like the Department of Homeland Security that focus on emergency response, defense, and security tend to have better resilience profiles than, let’s say, the IRS.

Right, so the public sector includes a huge array of organizations—from little towns to giant federal agencies like the U.S. Army or FEMA. When you think about resiliency across the public sector, what does that mean to you?

I look at resiliency through three lenses. Those are: avoidance of outages, response to an outage, and then the ability to be resilient without having an outage. It applies to every level of government. So whether it’s a physical loss of power, destruction of a datacenter due to some natural occurrence such as a hurricane, a flood or an earthquake, or a cybersecurity incursion, how quickly can you be up and running again? How fast can you get people back into their workplaces if they are required to be in physical presence with the system to do their job?

The second part of the definition is recovery, the speed to recover services that are lost. Resilience is all about putting together people, processes, and technologies that demonstrate redundancy and the ability to take a hit and keep delivering the services citizens expect.
Regardless of the emergency, we need the ability to respond to unforeseen events. We saw this during the pandemic, when organizations developed new applications and processes that allowed us to meet public needs in new ways. I’m talking about things like COVID testing sites and apps that track testing and vaccination status.

As we go forward, the old definition of resilience, which measured how quickly you could respond to an outage and maintain service delivery, needs to expand to include these other use cases.

You blame legacy systems for why the public sector might be behind the private sector, but the private sector deals with legacy issues, too. Is it the scale or mission of the public sector that explains why it’s behind?

In this time of COVID, if you have a business that has to send people home to work and it takes them two weeks to establish the VPN so that they can work from home, the business loses some money. If the government has a disruption that causes people to work from their homes and it takes two weeks to regain their capability to deliver citizen services, people may die.

So the urgency of the mission and the purpose of the organization is directly reflective of the type or level of services being provided in government.

People are relying on those services. And they’re relying on the government to have thought through resiliency, redundancy, recovery, and avoidance to be able to continue to deliver those services—and then actually deliver even more services when there’s an emergency.

It seems like people always prepare for the last emergency. How can the public sector prepare for unknown, future threats?

At every level of government, at the federal, state, local, provincial, and municipal levels, by their very nature they view the world through hindsight: Something happens? If either went well or it didn’t. Let’s have hearings and find out what went wrong and figure out how we’re going to fix it going forward. We have some really talented people in government who are thinking about the “what ifs” and they’re being very imaginative about what might happen and how we might avoid it, but then you run into the funding problem and the prioritization of programs. Now you compound that challenge with the issue of maintaining legacy technology. At some federal agencies, up to 98% of the IT budget is spent maintaining legacy technology. That leaves nine cents for innovation. On every dollar. That puts the challenge into some perspective.

Then when an emergency hits, like the pandemic, the money falls out of the trees. Right now, many agencies are flush and looking to spend money. How can we make sure that we get accountability? How can we manage the vaccines? How can we do this, how can we do that? And the agencies are responding very well. Most agencies have really stepped up.

COVID has accelerated the adoption of new technologies across industries and sectors. So to go back to the very beginning, is the stereotype that the public sector is behind still true? Could there be a cultural change going forward because of the pandemic?

In their understanding of the value of technology and their desire to provide the latest capabilities, they’re not behind at all. Almost every agency has a strategic investment plan to modernize their technology and processes, and to deliver the types of resiliency that we’re talking about.
Organizations need ‘privacy by design’

In today’s world, privacy safeguards must be baked into every process and product

BY EVAN RAMZIPOOR

Widespread digitalization has given organizations access to more data—and more types of data—than ever before. Businesses now routinely store massive amounts of information about their employees, customers, partners, vendors, and suppliers: onboarding and interview data, data from in-home smart devices, data about transactions, supply chains, and more. While data is the lifeblood of most organizations, it also poses a substantial liability. As countries, states, and cities continually pass new governance and compliance measures, the regulatory landscape is becoming increasingly difficult to navigate. Businesses are now beholden to a complex web of governance, risk, and compliance laws. And as hybrid and remote work become the norm, the threat landscape is growing and changing quickly. Companies are processing and storing data from new digital services that saw rapid uptake during the pandemic. At the same time, threat actors are changing their tactics in response to shifts in work habits.

For those responsible for safeguarding the ever-increasing volume of data and making sure their organizations are resilient in the face of such threats, how can they maintain an effective data privacy program?

To answer these questions, Workflow sat down with two senior managers at Ernst & Young—Ishant Goyal, senior manager and ServiceNow architect, and Tori Tripp, senior manager of data protection and privacy. Using the Now Platform®, Ernst & Young built automation tools that enable organizations to customize privacy-related workflows. When onboarding a new vendor, for example, instead of manually checking whether the vendor is using inventory software that is compliant with local and federal regulations, the system can help check automatically.

Goyal and Tripp believe the key to a good program is “privacy by design.” Rather than attempting to secure products and services after they’re launched, privacy by design bakes privacy protection into the development process.

What came out of this conversation were nine steps that executives can take to implement privacy by design in their organizations.

1 CREATE A CULTURE OF PRIVACY WITH STAKEHOLDERS

While the privacy team might understand the importance of security, other teams might not have the same level of understanding. Nevertheless, getting buy-in from the company as a whole is crucial. After all, it isn’t just the privacy team that keeps the organization secure—it’s everyone. Since
anyone could potentially fall prey to a phishing attack, store their data improperly, reuse passwords across devices and applications, or commit an error that leads to a data leak, everyone must be on board with privacy initiatives.

Educate leadership on the importance of strong privacy protection so that they can set the tone for the organization. No team, from marketing to sales to product, should have a conversation without talking about how privacy fits into what they’re doing. “Creating a culture of privacy starts with the leadership team,” says Tripp. “Getting leadership buy-in and having that tone come from the top down is crucial.”

CREATE CONSISTENT PRIVACY CONTROLS Privacy controls dictate how personally identifiable information is secured and how a consumer’s privacy is maintained. Since federal and state authorities are increasingly willing to regulate privacy and security protocols, proactive self-regulation is crucial or the organization risks having to play catch-up ad nauseam. And since the regulatory landscape is changing so quickly, it’s no longer efficient—or even possible—for larger organizations to manually change privacy in response. Organizations must create a simple, intuitive, and automated system for data privacy controls. Non-technical teams in manufacturing, business, and sales must be able to operate this system without consulting IT or privacy teams. The system should be embedded into each team’s work processes, so the company can easily stay compliant without adding friction for employees.

ENABLE CONTROL POINTS AND OPERATIONAL ACTIVITIES The consensus among privacy and security experts is that organizations must shift privacy and security left, meaning they should incorporate privacy safeguards as early as possible into their product-development lifecycle. It’s a consensus for good reason. It’s far easier to think about how a new system or product will protect customer privacy before it’s designed or shipped. Just as you should think about shifting privacy and security left in product development, it’s crucial to shift left operationally, too.

Think ahead about how and when your employees can—and should—access data. That’s where control points and operational activities come in. A control point is like a gate through which employees must provide credentials to “get in” and access data on the other side. Those credentials could be admin capabilities, passwords, user accounts, or policy configurations. Operational activities, sometimes called operational security, are risk management tools used by managers to evaluate operations from the perspective of a potential threat actor. Thinking about how a threat actor might exploit the system—before they actually do—allows for more secure IT infrastructure.

MANAGE POLICIES AND NOTIFICATIONS It’s helpful to think of specific policies and notifications as the tangible result of a strong privacy culture. Policies are the concrete rules that employees must follow in order to maintain data privacy culture. Policies are the concrete rules that each group can understand and support. The consensus among privacy and security experts is that organizations must shift privacy and security left, meaning they should incorporate privacy safeguards as early as possible into their product-development lifecycle. It’s a consensus for good reason. It’s far easier to think about how a new system or product will protect customer privacy before it’s designed or shipped. Just as you should think about shifting privacy and security left in product development, it’s crucial to shift left operationally, too.

Think ahead about how and when your employees can—and should—access data. That’s where control points and operational activities come in. A control point is like a gate through which employees must provide credentials to “get in” and access data on the other side. Those credentials could be admin capabilities, passwords, user accounts, or policy configurations. Operational activities, sometimes called operational security, are risk management tools used by managers to evaluate operations from the perspective of a potential threat actor. Thinking about how a threat actor might exploit the system—before they actually do—allows for more secure IT infrastructure.

INVEST IN DATA CLASSIFICATION STRATEGIES Organizations that process a high volume of data often lose visibility into the types of data they’re storing. If no one knows what data is being stored and where it’s coming from, then it can’t be secured. Data classification assesses the data that an organization has stored and figures out whether it’s properly secured. New tools and technologies make this a simple and effective process. For example, BigID, a data management company, makes online tools for managing private data. Tools like BigID connect to the company’s network and parse its data into types, so ex-ccx can decide which controls must be put in place to secure company assets.

PREPARE FOR PRIVACY INCIDENTS NOW Security breaches and data privacy incidents will occur. When managing high volumes of data, breaches are inevitable. The first step to managing them is to acknowledge that reality. Rather than aiming to plug every vulnerability in the system, build in processes to prepare for privacy incidents. In the event of a privacy incident, move quickly and transparently. To that end, it’s a good idea to prepare the response and to practice responding to test incidents and scenarios as often as possible. In addition to responding to the incident itself, do root-cause analysis to figure out how it happened, which regulations apply to the incident, and what customers need to be notified. Prepare for a surge of data privacy requests post-incident; customers will want to know exactly what happened and whether they were impacted.

PLN FOR CUSTOMER DATA REQUESTS The General Data Protection Regulation (GDPR) gave EU citizens, and anyone who does business with EU organizations, new rights to data access and privacy. Under GDPR, such individuals can make a “data subject access request” (DSAR) to learn what an organization knows about them and how the company uses that information. The California Consumer Privacy Act (CCPA) establishes a similar right, and other states are in the process of passing acts that enable consumers to make a DSAR as well.

CREATE A CULTURE OF PRIVACY STARTS WITH THE LEADERSHIP TEAM.”

TORI TRIPP, SENIOR MANAGER OF DATA PROTECTION AND PRIVACY, ERNST & YOUNG

When planning for DSARs, there are two things to keep in mind: regulatory requirements and user experience. On the one hand, GDPR, CCPA, and other regulations govern how and when companies must hand over user data or face fines and other legal actions. On the other hand, a data subject privacy request is an opportunity to establish trust with users. By making the process as fast and smooth as possible, you can show your users that you’re invested in their privacy and security.

Responding to such requests is a complicated, multi-step, cross-functional endeavor. Organizations need to create response systems now. Such systems should automate responses so the process is streamlined and efficient, or companies will be overwhelmed by requests and face rate users.

MANAGE THIRD-PARTY RISK The rise of supply-chain attacks such as the high-profile SolarWinds incident has made third-party risk from suppliers and vendors top of mind for many businesses. Before engaging with a supplier, client, or vendor, it’s crucial for organizations to think about such risks. Rather than kicking off a deal with a vendor and applying privacy controls post hoc, build risk assessment into the processes used to interface with third parties from the get-go. These assessments should cover the scope of data that third-party providers are allowed to handle, what they should not handle, and what they need to do when a breach occurs. “It’s almost like a vendor assessment,” says Tripp. “It enables you to ask whether your suppliers are meeting certain regulatory requirements.”

Risk assessments shouldn’t end when a contract does. In fact, after ending a contract, companies should perform an audit to ensure the third party deletes any data that no longer belongs to them.

LEVERAGE AUTOMATION The automation tools like those that Ernst & Young built using the Now Platform® enable organizations to customize privacy-related processes that work for their business. They help automate processes, workflows, risk assessments, best practices, and frameworks—the building blocks of risk assessment and data privacy. Once you bring privacy into existing processes and products is too complex to handle manually, automation tools play a substantial role in implementing and automating privacy by design.
“Ikigai” is the future of work

HOW AN ANCIENT JAPANESE PHILOSOPHY COULD HELP CREATE HEALTHIER, MORE CONNECTED WORKPLACES

BY CHRISTINA LEE

The Japanese island of Okinawa has the highest concentration of centenarians in the world.

The longevity of Okinawans is often attributed to their diet and their close-knit community. Their diet is mostly small portions of vegetables, fruit, fish, and grains, light on sugar and salt, and ample amounts of green tea and antioxidants. Their neighborhood associations, known as “moai,” are key to the island’s robust social safety net, which makes sure everyone is cared for and has something to do.

Underlying the relaxed and supportive lifestyle of the Okinawans is their belief in the Japanese concept of “ikigai,” or “reason for being.” Ikigai embodies the notion that each person has a specific reason for being alive and that part of life’s journey is to discover one’s ikigai and live it fully.

Ikigai has been offering vital life lessons to the Japanese for more than 1,000 years. It offers us a rich, humane perspective on life and work. Ikigai teaches people to embrace life, including eating right, staying healthy, and keeping busy.

The story of Okinawan longevity and the importance of ikigai in their lives is explored in the international best-selling book “Ikigai: The Japanese Secret to a Long and Happy Life” by Héctor García and Francesc Miralles. The secret they unveil is also instructive to companies and employers who see the connection between highly satisfied and empowered employees and greater business value.

Making sense of ikigai: life, value, and worth

Ikigai is centered around the why of life—giving meaning to what one does and how one lives. This philosophy focuses on four broad areas to help derive meaning—all of which apply to both our personal and working lives. It asks us to find a sweet spot where what you love, what you’re good at, what the world needs, and what you can get paid for all meet.

Identifying your ikigai is just the beginning. Identifying and achieving are two separate things. It is a lifelong journey to identify and then fulfill one’s ikigai. Resilience in this context means staying focused on the long-term goal. It also means having the strength and fortitude to get up and try again after you fall. Dealing with setbacks and responding to change is vital to realizing one’s ikigai. The ability to identify and deal with setbacks, changes, and new situations is all part of the journey.

Finally, unlike typically Western, individualistic philosophies, ikigai focuses on how a person fits into their community. Finding one’s ikigai means finding one’s own path and understanding how it will impact family, neighbors, fellow employees, or fellow citizens. The result of chasing these worthy ambitions can have far-reaching effects, especially in the workplace.
4 ways to build ikigai in your workplace:

1. CREATE BALANCE
   Good work comes from a shared mission, not a shared location. When you give employees flexibility and a good work-life balance, you empower them to create sustainable value on their own terms.

2. LOSE THE BUSY WORK
   Employees typically spend much of their time doing routine tasks. This leaves little time for innovation and value creation. By simplifying processes and digitizing workflows, companies can unleash the creative potential of their workers.

3. HELP EMPLOYEES HELP THEMSELVES
   People need easy answers to their questions to stay productive. Providing a strong Q&A knowledge base, self-service tools, and access to community insights gives workers the ability to solve their own problems, better serving themselves and, in turn, their customers.

4. GROW THE TALENT ENGINE
   Technology investments can’t produce ikigai on their own. It’s just as important to invest in your employees. To succeed in the modern workplace, they need training in soft skills and business best practices, along with data analytics, app development, and other tech skills. A sustained focus on training can boost performance and create better experiences for customers and employees.

Workflow Quarterly
is published 4x/year. ©2021 ServiceNow. All rights reserved.
Fuel business agility and resilience

Drive growth, strengthen business continuity, and enhance employee productivity with the Now Platform.