VIPRE SECURITY GROUP

Expert Insights

The Three Pillars of Cyber Security

People, process, and technology are often mentioned as part of the key approaches to defending an organization against the rolling, turbulent seas of cybersecurity.

However, should each of these fundamentals be treated as mutually exclusive? That is, does conquering any one prong of this trident mean that the others can be disregarded? Similarly, can an organization be considered secure if any of these fail?

We interviewed 16 cybersecurity experts

to learn their views about each of these topics.

Their insights offer interesting examples of what they consider the most important of the three pieces. Are they separate entities that function autonomously? Is integration possible? Is there a defining line where one factor ends, and another begins, or do they blur into each other?

Find out what the experts had to say by looking inside.

People

When it comes to the People, Process, and Technology (PPT) framework, what is the People part all about and what are organizations getting wrong?

Zoë Rose
IS Lead, Canon EMEA

John Trest
Chief Learning Officer at VIPRE Security Group

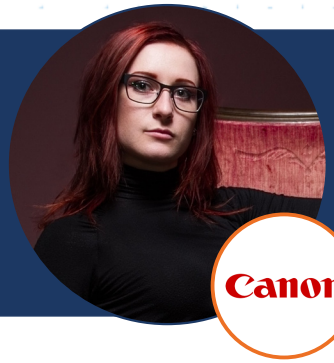
Chloé Messdaghi
Chief Impact Officer, Cybrary

Goher Mohammad
Head of InfoSec, L&Q Group

Kassia Clifford
Infosec Consultant,
Kassia Clifford Consulting

Lee Scorey
Founder, Consultants Like Us

People



Zoë Rose

IS Lead, Canon EMEA

> *"The difference between a mediocre organization, and an excellent organization when it comes to security, is through enabling people."*

When we talk about people, process, and technology, we often focus on technology; on solutions. This is ironic to me, because people are first and, actually, people are the most important part. People are an organization's greatest asset; technology only goes so far.

The most important part of security is the security culture; it's the people understanding why security is important, and how to apply it. In an organization, that culture is created by not only how the organization teaches why security is important, but how the organization practices security.

Awareness has to be mixed with practical application, but, too many organizations throw money at the problem, react to incidents without a formal root cause or lessons learnt, and assume the default annual training everyone takes is good enough. Those foundational gaps stop them from improving.

Addressing phishing is important because it continues to be a top threat to organizations across industries. Remember, malicious actors are assessing their own return on investment - how risky the task is, and the difficulty of the task, versus the benefit to them. Phishing, whether targeted, or just a general email blast, is an easy task for cybercriminals, offering maximum benefit with little chance of identifying the attacker. The strongest motivation of phishing schemes is financial gain.

People

Zoë Rose | IS Lead, Canon EMEA

The most lucrative target is a person who works on the finance team, especially when the attack method exploits a part of their normal role; opening attachments, and clicking links. This emphasizes the need to address that aspect of “why” and “how” to apply security to their role - if the training is centered around telling them to not click on links and to not open attachments, all that’s going to do is create a culture where they ignore the training, because it doesn’t allow them to do their job.

Instead, the training should be tailored to address these concerns, and it should teach how the organization pragmatically protects itself, and where the responsibility lies with the team. It is also important to address how to report, and to ensure the establishment of a no blame culture. More weight should be given to the successful reporting of a malicious link, than treating the clicking on a link as a failure. This will help people feel safe to admit when things happen.

Another common security culture challenge occurs when policies are created in a vacuum, without talking to the people who are directly impacted by the initiatives. This often causes issues with their workflows, because never have I found an organization who perfectly documents every single requirement, every single change. They try, but nothing is perfect, that’s why user acceptance testing and validation is needed.

For organizations that are trying to improve their security posture, the first topics they need to focus on is collaboration and communication; building that trusted relationship. Senior leadership needs to trust their security team. They each need to work together.

People

Zoë Rose | IS Lead, Canon EMEA

> *Historically, this industry has spread a lot of FUD - fear, uncertainty, and doubt.*

The reason it's so hard to teach about security effectively is because it has such a negative connotation. Historically, this industry has spread a lot of FUD - fear, uncertainty, and doubt.

To overcome this, we have to ensure that our colleagues understand we listen to their needs, prioritize them as well, and are collaborating to create a secure and effective approach.

To do this, they have to trust us. To build that trust, we have to listen, we have to empathize, and we have to adjust to their needs as well. We have to create a culture that intrinsically wants to follow workflows that may be different, but still allows the job to be completed.

If an organization is able to prioritize it's people, working together to create an environment that security is almost transparent to end user experience, then it's going to stand out as one of the best.

People

Chloé Messdaghi

Chief Impact Officer, Cybrary

> *"The best way to make people the strongest allies in security is in how we train or how we educate them."*

If you're not listening to your people, that means that you're going to take actions that are going to result in a risky and unpredictable situation for your organization.

"People, process, and technology" is a simple concept. However, many organizations do not always get those right. One area of deep concern is the "people" part of the equation. What is that all about and what are our organizations getting wrong when it comes to people?

The reason that it's in that order – people, process, technology – is because people are running security. People are also the ones who are going to click on a link and can be the threat inside your organization.

The people part of it is to acknowledge that you cannot fully rely on technology to keep you secure. You need to also rely on people because they're the ones who are creating the technology.

The best way to make people the strongest allies in security is in how we train or how we educate them. You first need to make sure that they're passionate about it. We always hold the assumption that we will just present the information, and we're good to go. The reality is that when you're teaching people who haven't been involved in a breach situation, they may treat security apathetically.

People

Chloé Messdaghi | Chief Impact Officer, Cybrary

The main thing that organizations are getting wrong is to understand that when we're teaching people, or training, it is an ongoing process. It is a continuous up-skill.

One of the most important points when driving a people-based approach is that you have to invest in your people. If people don't feel like they're being invested in, then why should they care about securing your environment, or why should they care about double-checking every time someone sends an email and whether or not to click on an attachment or a link?

When we don't invest in people, then we're going to deal with people who are struggling with burnout in the end. Burnout happens not necessarily because of being overwhelmed with work. The reality is that burnout comes from a lack of organization, caring, and poor leadership.

People

Goher Mohammad

Head of InfoSec, L&Q Group

When speaking about the people aspect of “people, process, and technology,” what many people and organizations get wrong is referring to others as “the weakest link”. I really don’t like using that ideology. To characterize it in such a negative way always makes people feel a bit stupid.

My approach is that security should be invisible. It should be something that’s part of what people do, and they don’t even realize they’re doing it. People in organizations have a focus area, whether it’s Finance, or it’s Human Resources, or Technology; whatever it is, that’s their goal. Security is not their goal.

Incentives are really important. If there is an incentive, people are going to be more encouraged to do what is right. Rather than reprimanding people for making a security error, we have to ask how we can better engage them. We need to be in a place where people who report phishing, or report incidents are encouraged with an incentive; they get a voucher for a coffee, or, if there is no budget for a monetary incentive, they get some other tangible encouragement. That positive enforcement is a really good way forward. It also serves by giving people something back. If they learn something from it that helps them in their personal lives, that is really important. Whatever training is given to them should help them in their personal lives.

People

Goher Mohammad | Head of InfoSec, L&Q Group

The workplace has changed dramatically. The ability for people to work from wherever they are presents a big trust element. There has to be trust on the people side of it. Then, you encapsulate good practices and processes around that in the technology.

It's in empowering employees and people to do the job they're meant to do, and then giving them the right environment to do that within a secure place, from a security standpoint. It doesn't really matter where the location is. As long as you empower your staff with the right environment, which is secured in the right way, and they're trusted to do their job, then everything moves in a really good direction. There are some security challenges, but there are also some great solutions out there to help with those security challenges.

Training techniques should be moving along with the times. People love short-form information these days, such as YouTube and TikTok videos. Everything's just a lot more bite-sized, and a little more "snappy." Attention spans are smaller, so we need to work in that direction. Our training methods should be similar. Rather than flooding a person all at once with a long, often tedious training, they would probably benefit more from a series of short videos, spaced throughout the year. This may even spark increased interest in learning more about security as a general topic.

People

John Trest

Chief Learning Officer at VIPRE Security Group

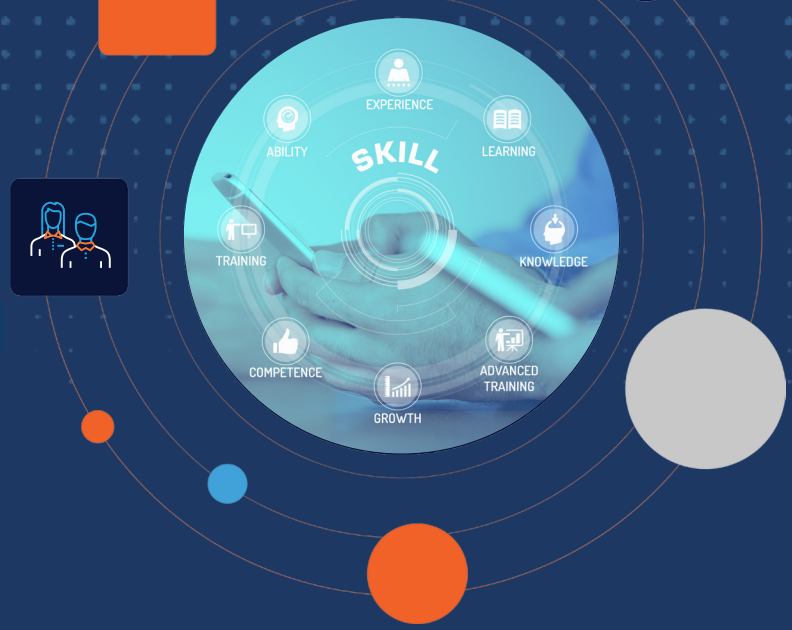
When it comes to security awareness training, one of the main weaknesses is that the people who are typically tasked with that responsibility are the security team.

Yet, that creates a strong disconnect, as they have specialized knowledge in security, but they are usually not professional educators. And, in small organizations, it might be difficult for the security staff to potentially partner up with someone who is more familiar with adult learning, potentially, the Human Resources or Learning & Development departments. For an effective security awareness program, it's important to get other people involved who can provide the necessary adult learning expertise and support, including any external training vendors.

> *"Training should be inclusive. You have diverse workplaces, diverse people, and they need to understand how security awareness affects their day-to-day lives. They need real-life scenarios and diverse imagery that reflects themselves and their work environments in their training. This allows the learner to really put themselves in the position of the people in the courses and simulations. To get the most impact from the training, the employee really needs to be able to relate to these situations."*

People

John Trest | Chief Learning Officer at VIPRE Security Group



Establish areas in the training to really motivate the employee such as establishing how the material is valuable to the organization, certainly, but also to the employee and their loved ones.

Once you have their attention and focus, make sure that the material is relevant to them. Case in point, when you talk about malware, you should explain the symptoms and characteristics, and how to report it. That's very important because that's going to be relevant to their day-to-day experience, as opposed to teaching what may be irrelevant subject matter for them, such as going on and on about Advanced Persistent Threats (APTs), or the history of malware. The material has to be relevant to how they can implement these security best practices in the workplace as well as in their own lives.

There are lots of different factors that impact how you successfully train an employee. If these factors are not considered or implemented correctly, then the training is not going to have the impact and the effectiveness that is required to really provide a proper defense. Really understanding who your audience is, and how they work is very important for success.

There are many things that you can offer to reinforce the messaging and the security best practices, so that employees remember and are able to apply what you are teaching them. Done correctly over time, that information becomes strongly established in the person's mind, so they can provide a proper defense for your organization.

People

> *Oftentimes, we hear sales is everybody's job. I'd like to expand that to include security as a part of everybody's job.*

Kassia Clifford

Infosec Consultant,
Kassia Clifford
Consulting

Too often, we dehumanize the people that are actually involved in your security program. Although humans are imperfect; they are intelligent and can be highly engaged if you help them. When armed with the right tools and a process, your team is unstoppable in supporting a security department and program and achieving their goals.

Many organizations don’t see security as a business driver. I think that is changing in part because of the working model brought about by the pandemic, and the associated demand for proof of an organization's security posture. Often, the business leadership has not created space for the technical leaders to influence security strategy. This is an imperative step to generating buy-in from those who will carry out the security work. It is also tough to do when pressures to continue developing and maintaining a product or service are so dependent on these technical leaders.

People

Kassia Clifford | Infosec Consultant, Kassia Clifford Consulting

When I think of how to create a better security culture, I keep in mind a phrase that my uncle once said to me: "The fish rots from the head." So, what that means is, if we do not have executive buy-in at the very top of an organization in your security efforts, it's not going to trickle down to all of your control owners and employees. Ensuring executives are champions of security is key.

There also needs to be strong alignment between human resources and security. Teams know that performance reviews aren't going to be impacted because of the existing security posture. Only after a program is in place, employees are trained, and gaps are outlined and addressed, can security activities be tied into your performance and your role, especially when you're in a leadership position or you're control owner.

The way that I see solving a lot of these problems is two-fold. For business leaders, they need to ask questions, and be educated in that which the security team is trying to accomplish. The security function is to create processes and culture, to secure the organization. If you don't agree with their approach, have a conversation about it, rather than trying to circumvent security. We need leaders to set an example and be champions. The security team can reciprocate by staying out of the weedy details until asked for those details.

If we blast all of the information at once, no one hears anything, brains shut off, egos slow down, and employees are just sitting in judgment, wondering why we security people don't know how to communicate properly.

People

Lee Scorey
Founder,
Consultants Like Us

"Even a fully autonomous organization has a dependency on people. It's people that ultimately buy their products or services, so there is no getting away from the fact that you need people in order to function."

We have created too many choices for our staff by providing a wide range of software, and all of it is available for us to access from the comfort of our homes.

We install new software enhancements without understanding whether we need to – yes I know some software needs upgrading to maintain security.

We roll out software without actually explaining how to use it. Often, staff are simply left to figure it out for themselves, they are left to turn to tech and other users of the technology to figure it out.

People

Lee Scorey | Founder, Consultants Like Us

Create ‘Process guides’ that are easy to follow. No one wants to read a 300-page manual about how to use an application (ok, some of us do). But the average person needs to know how to get started, what their limitations are, and who to turn to for help when they have a problem.

Top tip - create flowcharts for your processes. They are much easier to follow.

And finally, look after your staff and check in with them. Check that they are not working on back-to-back meetings. The theme here is well-being. If staff feel like they are truly being looked after, they will look after you.

Process

Adrian Sanabria
Director, Tenchi Security

Angus Macrae
Head of Cyber Security, King's Service Centre

Amar Singh
CEO, Cyber Management Alliance

Ian Thornton Trump
CISO, Cyjax Limited

Usman Choudhary
CPO, VIPRE Security Group

Ross Moore
Security Analyst, Passageways

When it comes to the People, Process, and Technology (PPT) framework, what are some of the key benefits of having good Processes in place? What advice would you give to those who might be looking to implement new, or different, Processes into their cybersecurity strategy? And why is Process so important when it comes to connecting People and Technology?

Process

Adrian Sanabria
Director,
Tenchi Security

Process is absolutely the missing link - it's the glue that holds everything else together. Without it, people, technology, and the security programs based around those simply fall apart.

I strongly believe that process failure is the top reason that breaches occur, fail to be prevented, or fail to be detected. In most cases, the organizations had the people they needed and the tools they needed. However, the staff wasn't well trained on how to use tools or how to perform investigations. The tools were misconfigured, documentation and asset owners couldn't be located, there was no usable software inventory, attack detections were created, but never tested before being deployed to production.

Practice is the key here. A sports team that has all of the equipment they need, but has never practiced, cannot win a game. The same is true in security. Any organization hoping to detect or repel even mediocre attackers should probably be running live simulated attacks at least once a month.

> *"Practice is the key here. A sports team that has all of the equipment they need, but has never practiced, cannot win a game. The same is true in security."*

Process

Angus Macrae
Head of Cyber Security,
King's Service Centre

It is important for anyone looking to implement a new or different process into their cybersecurity strategy to think more strategically about the wider purpose and desired outcome.

When it comes to the people, process, and technology, processes should provide structure, order, and a repeatable, united approach to conducting important activities.

For example, good security Incident Response (IR) processes should provide a vital sense of order, not only for the people responsible for technology during such high-pressure circumstances, but those with data governance, legal compliance, or communication responsibilities as well. Without these, well-intentioned but disjointed and possibly duplicated actions will reduce the efficiency of a response.

> *"The key benefits of having good processes in place may mean rather different things to different people and areas of an organization. The benefits of well-defined processes should however be apparent and appreciated from varying perspectives."*

Process

Angus Macrae | Head of Cyber Security, King's Service Centre

From a management perspective, a good process should give confidence in efficiency, productivity and repeatable outcomes, helping to minimize resourcing effort and risk. From an audit perspective, it should provide some assurance that core functions are being run professionally and with due care. From a financial perspective, it should help to demonstrate how essential activities are being delivered without carrying unnecessary waste or cost. Operationally, it is absolutely vital that processes are understood and consistently applied to ensure the correct running of critical enterprise technologies. For the technical IT staff responsible for such systems, it should provide them with benefits of security and protection, ensuring that they are "following the correct process" when conducting a necessary but higher-risk change, for example.

Even with the continual push towards increased automation, processes need to be well-defined, proven, and appositely optimized before attempting to automate them at any level. The old adage that you should "never outsource a mess" applies here. Neither should one attempt to automate a broken process and expect that alone to fix it.

Process

Amar Singh

CEO, Cyber Management Alliance

It is important to have that open atmosphere to let people critique the process and improve it.

Process is often neglected. Technology is abundant in terms of availability. There are new and different technologies coming out every day. Processes, however, are always assumed as boring and already in place. The question that must be asked, is, do my staff understand the process, and are they actually happy with the process? Because, let's be really brutally honest with ourselves, the majority of smart humans will find shortcuts if the process is too complicated. If the process can be accomplished in an easier way, then the complex version appears completely useless.

> *"Why do I have to perform 50 steps to achieve an objective that I can do in two steps?"*

When you ask a person, or a group of people to operate a technology or to achieve an objective, and you create a process with documentation that's either too complicated to read or understand, then it should not be surprising that they may not proceed correctly. Writing documents is brilliant, but people need to understand a process. The audience should also be given the opportunity to voice their comments and suggestions to improve that process.

Process

Amar Singh | CEO, Cyber Management Alliance

One of the questions I always explore is, have my actual operators reviewed that process? Have they performed the process three or four times? And furthermore, what suggestions do they have to improve it?

It's the people who use that process who know it best, and who can help to make it better. Many large and medium size organizations forget that the operators of the process are the best sources to continually improve it because they're doing it so many times. They are the ones who may be able to show how a process can be achieved with the same results in less time. A smart organization would give them a voice where they feel that they have an absolute input into the optimization.

> *"The IT and cybersecurity industries are plagued by complexity. The question that should precede any new process is, why is the process there if you don't know the desired outcome of that process? You may have a process in place to meet compliance, but does it actually help keep an organization secure?"*

Process

Ian Thornton Trump

CISO, Cyjax Limited

Good process can really help in making your security control investment operate far more efficiently, and the organization may be able to automate a well-documented process which, not only is efficient, but will be far less prone to human mistakes.

Processes are key to the implementation of an effective cybersecurity strategy, but why are they so important when it comes to connecting people and technology? People need to be aware of online risks, threats, and how they may be targeted. Processes need to be documented, and controls put in place to detect aberrations. When it comes to robust cybersecurity, the combination of aware people and documented process is nearly “the whole security thing.”

“Processes are key to the implementation of an effective cybersecurity strategy, but why are they so important when it comes to connecting people and technology?”

Process

Ian Thornton Trump | CISO, Cyjax Limited

When it comes to people and process, everyone should be on the lookout for situations where they are being manipulated or coerced to deviate from a documented process and – this is critical – an escalation path for security issues if they are unsure.

The key benefits of having good processes in place is really about being able to detect digression from normal business activities at an end-point level, and also at an organizational level. Consistence of behaviour allows for far better telemetry identifying “security signal” from “security noise”. This is critical for identifying fraudulent activity, as well as malicious activity within the organization. If everything is generally following a process, then the output should be fairly consistent.

Process

Usman Choudhary

CPO, VIPRE Security Group

Process is critical to having both an efficient and effective security posture.

When we talk about cybersecurity, we often hear that it is about people, process, and technology. These three topics are usually treated as separate entities, and they can certainly stand alone, each having a specific function in the overall security strategy. However, they also operate together to form an efficient security program. If we examine processes alone, we see that they are the key to implementing an effective cybersecurity strategy, but why are they so important when connecting people and technology?

There are a couple of angles to connecting these. First, we know that many security incidents are the result of misconfigurations. Process can help formalize how technology is configured and used to avoid these pitfalls. Defined processes have great importance. For example, onboarding new cybersecurity staff poses the risk that they may not be familiar with the tools used and are likely unfamiliar with the risks to that particular company. A good process, especially with excellent documentation, is one way to prevent a misconfiguration from creeping into the organization.

Process

Usman Choudhary | CPO, VIPRE Security Group

Another way to connect people to process is through security awareness. Process is vital to the success of employees becoming aware of security risks.

In that context, when we present training or phishing simulations, there must be an effective training program and process where cybersecurity meets the staff. They all become part of the organization's cyber effectiveness and program. Once a year training is not enough. You must have continuous learning and learning management around the whole process, both from a risk reduction perspective and general awareness of how to deal with security incidents effectively.

The best way to see if a specific tool is a good choice is to design a holistic overlay process that complements the tool and the controls being put in place. The tool alone is not the security solution; it's the tool, along with the process and the ability to maintain that tool over time, that protects you from cyber threats and risks.

People think the foundation is technology, but it's more than that. Process is the glue that connects interactions between the people in your organization and the technology, i.e., the devices, resources, and assets that you're trying to protect.

Process

Ross Moore

Security Analyst, Passageways

People, process, and technology" (PPT) is like a three-legged stool, or a triangle - each is useless, even detrimental, without the other two.

People are the "who," technology is the "what", and processes provide the "how." Processes enable security professionals to make the right technological decisions. However, unless professionals are in a leadership position to create and drive the guidelines and procedures, then they need those processes so they can do their jobs. It's not that the leaders are incapable, but that guidance directs them about how to produce what the business needs, given the technology that's available.

With good processes, professionals can determine if they have the right technology. Does the process goal fit in the current technological parameters? Or does another technology need to be procured to reach the goal? When viewed that way, it appears that processes keep technology in its place. Another important point is that processes are for people, not the other way around. When the people change, e.g., workforce upheaval, or a change in business priorities, the processes likely need to change. Don't make processes that lord over people. Processes are a business tool; they're not leadership or management.

> *"Another important point is that processes are for people, not the other way around."*

Process

Ross Moore | Security Analyst, Passageways

There are some key benefits of having good processes in place. One is that processes can provide a solid succession plan. When important people, or if whole departments leave an organization, processes help smooth the transition to new personnel. Other ways that tangible benefits are realized through good processes are in businesses stability, reliable metrics, and consistent workflows.

One of the best ways to make people, process, and technology work as a unified force is by having a security leader who has a seat at the corporate leadership table. It seems cliché, but that leader who has the strategic, tactical, and operational expertise - along with the proper management and people skills – can be the catalyst for integrating business and security initiatives, and moving corporate security onward and upward. That integration provides the PPTs needed for security professionals to accomplish what they need and want to, which includes supporting the business, growing their skills, increasing their reputation, and having a fulfilling career.

Technology

When it comes to the People, Process, and Technology (PPT) framework, what do you need to consider when looking at Technology to secure your organization? What are the drawbacks of leading with a Technology first approach, and what advice can you share with other security leaders when looking at the Technology part, in conjunction with People and Process?

Hunter Sekara
Security Engineering,
CACI International

Mandy Huth
VP of Cybersecurity,
Kohler Co

Christos Sarris
Information Security Manager,
Sainsbury's

James Packer
Head of Information
Security, EF Education First

Technology

Hunter Sekara

Security Engineering,
CACI International

While technology can add value, organizations should avoid a technology-first approach to cybersecurity.

Technology is dynamic, and new tools and products arecontinuously being developed Technology should not lead or guide an organization's security approach. Instead, organizations should start with the fundamentals such as access control, auditing, configuration management, identification and authentication, and secure communications and supplement those areas with products that fit the organization's unique needs.

Start with the basics and the organization's unique business and security requirements, and then find solutions to fit your needs. Consider the risks associated with your assets, analyze the risks, perform a cost-benefit analysis, and then choose cost-effective solutions to achieve proportionate levels of security.

Technology

Hunter Sekara | Security Engineering, CACI International

When considering people, process, and technology, try not to focus solely on technology. Although technical measures can help detect and prevent cyber attacks, we must not forget people and processes.

Remember, technology and people are continuously evolving. While technical skills can be advanced with training, soft skills and behavior are more challenging to influence based on an individual's beliefs, perceptions, experiences, and attitudes. Consider framing the mission and business implications of a security attack to employees to gain buy-in and advocate how people, processes, and technology work as a cohesive whole to enable the organization to achieve strategic objectives. When a holistic understanding of security exists within the organization, there is a greater likelihood that security will be considered throughout all business units.

"...advocate how people, processes, and technology work as a cohesive whole to enable the organization to achieve strategic objectives."

Technology

Mandy Huth

VP of Cybersecurity,
Kohler Co

Technology is really important, but it can't be the only thing we think about.

Technology is really critical to any business, but it has to occur in the right order. Many companies introduce technology that attempts to solve a problem, but that creates a "Band-Aid" effect. We need people, process and technology, and it should be in that order.

Conceptually, it's simple, but it's not always easy to live up to that ideal. If you don't have the people that understand the business and what they're trying to accomplish, if you don't have a process that really makes sure that you're doing what the business needs, the technology cannot be an enabling function.

> *"You can have the best technology in the world, but if you don't have someone to run it, and you don't have a process that supports it, then how is that technology ever going to be successful?"*

Technology

Mandy Huth | VP of Cybersecurity, Kohler Co

If you introduce a new technology, you must consider what prerequisites are needed across the enterprise as well as the downstream impacts of introducing that technology. When you have an enterprise architecture function, they can see across your ecosystem and make sure that the technology that you're bringing in is either going to be compatible, is going to have dependencies, or just isn't right for your ecosystem. It is really important that you think about it.

You need a platform that offers what I refer to as "microservice capabilities." I don't want to a single entity containing all the capabilities. I need components that I can break off and move, multiple Lego pieces that build structure. It really can be capabilities that I can get on – if not a single pane of glass – at least less panes of glass. So, I look for vendors and technologies that have more than one capability that will solve multiple problems. If I can reduce the disparate vendors to the lowest possible number, that gives my team the ability to focus on other value-added activities, rather than just the overhead of context-switching and moving to another pane of glass to look at something else or something very similar. Technology that has multiple capabilities, but isn't a singular monolith offers the best value.

Technology

Mandy Huth | VP of Cybersecurity, Kohler Co

Technology is a great, great thing. It just needs to be designed securely, and it needs to be managed, maintained, and audited for configuration drift. Most of all, it has to be thought of in partnership; in your people, process, and technology. Focusing on what problem you are solving, using process to solve that problem, and using technology to enable that process, will ensure your long term success.

Technology

“No matter how advanced a technology is, it cannot solve any business challenges by itself. We need to have the correct resources (people) and processes in place to dictate and drive its operational support, which will then help in addressing any of the problems.”

Christos Sarris
Information Security Manager, Sainsbury’s

I’ve seen many organizations out there that follow the people, process, technology concept in reverse (or only focus on specific parts of it), by first attempting to address technology before processes, and then saving the people pillar for last.

This approach creates the repetitive scenario of an organization investing a significant amount of money on a technology, which in practice is being unutilized and underused. It also creates a false sense of security, if we are talking about using a security related technology. People that have a passion for technology can very easily become fascinated with the advertized capabilities of the latest technologies, and very frequently don’t think about how the technology will integrate with other technologies within an organization and, most importantly, how it will improve its processes.

Technology

Christos Sarris | Information Security Manager, Sainsbury's

Some organizations are better at supporting change than others, and a drastic change to the technology pillar may have a very negative effect to people and processes. We always need to keep things simple; start from something small and simple and build on it.

> *"Be very clear about what you want to achieve by using a technological solution, and don't neglect the human factor. A lot of organizations during their digital transformation journey focus on technology and processes, and completely overlook the people involved in the change."*

You cannot drive change without the buy-in and support of your people, and our approach should be looking at long term impact versus the short-term (possibly positive) changes.

Remember that people do all the work, and well defined processes can help to increase the efficiency of our people, and then technology can introduce innovation (used by our people) and automation (for our processes). By looking closely at these three areas, including a fourth one, which is culture, we can then review current technology we are using in our organizations and make sure that we are using it to its fullest capacity. Very often, we can address parts of these four key areas by technology we currently use.

Technology

James Packer

Head of Information Security, EF Education First

Ultimately, the premise of the people, process, and technology philosophy is to consider all three pillars on equal footings – prioritising one over the others inherently will result in gaps in your risk landscape, either in your awareness/understanding of risk, or the successful treatment/management of that risk.

Technology seeks to highlight the relationship and intersections of the pillars of business that leverage data and information. Technology is a core part of the PPT concept. It speaks to the fact that, without a relationship to a process or a person, stand-alone technology is useless.

It also highlights that the vectors of threats and risks to technology originate from and emanate to people and processes. Ultimately, it is people and the processes they define that develop technology in the first place, both of which are by nature imperfect.

Technology

James Packer | Head of Information Security, EF Education First

It is important to understand that technology will not solve all problems – and be wary of those that claim to, or claim to offer "holistic" solutions. It is widely accepted to follow the phrase "the right tool for the right job" when choosing technology, particularly in the security sphere.

It's also important to educate yourself, not just in the "under the hood" mechanisms of the technology, but also the considerations from a legal, regulatory, or compliance lens of different types of technology and their operations. This is particularly important when working with cloud solutions that span multiple physical jurisdictions.

> *"Automation is most certainly a help in cyber security, simply put, because we currently (and won't for some time) have enough people to meet the cyber demands around the world. Not only does automation help fill gaps we have with an absence of staff/budgets, but it can protect the resource we have in place today, addressing alert fatigue, and eliminating monotonous, repetitive tasks."*

Conclusion

As you can see, the three attributes that form a comprehensive cybersecurity defense are people, process, and technology. What does this mean to an organization, and what do the experts' views offer to help against the constant threats that continue to emerge?

The integration of the three are vital to the best defense possible for an organization. However, as discussed by the experts, this is not a simple task. It requires more than just a mechanical approach. Integration of the three requires a human touch, coupled with logistical acumen, and technical skills. One obvious revelation is that no single person should be expected to achieve such a lofty goal. In fact, it is clear that, when speaking of people, process, and technology, the sum of the parts is infinitely greater than the whole.

Understand your cybersecurity better

VIPRE Security Group's free survey helps you to take a reflective look at your current security understanding benchmarked against well-known best practices. This can help you to better protect your organization against existing and emerging threats, as well as give you peace of mind around what you are doing well, and information to understand where you could easily improve. To take the survey and have a Cyber Security Assessment Report sent directly to your email go to https://s.pointerpro.com/viprecsassessment

Or to go to our full Resource Kit which houses additional interesting insight into the role People, Process and Technology in cyber security today.

Click Here

VIPRE SECURITY GROUP

SECURITY SERVICES FROM VIPRE


Endpoint


Email


Training


Network

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+ 45 7025 2223

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580