AT&T CYBERSECURITY INSIGHTS™ REPORT

AT&T Business

AT&T Cybersecurity

2022 SECURING THE EDGE

FOCUS ON MANUFACTURING

FOCUS ON MANUFACTURING

About This Report
This report is a special industry report with a focus on manufacturing. It is derived from the quantitative and qualitative research and analysis conducted for the 2022 core AT&T Cybersecurity Insights Report: Securing the Edge. For additional information and detail about securing the edge, we encourage you to read this industry report as well as the core AT&T Cybersecurity Insights Report.

Manufacturing Report Methodology Overview
This manufacturing report is based on the AT&T Cybersecurity Insights Report: Securing the Edge, published in January 2022. The report is based on data from a global survey of 1,520 security practitioners, IT practitioners, and operations leaders. It was conducted during September 2021, and respondents span a variety of market segments that are nearly equally represented at 16.4%: manufacturing, healthcare, finance, retail, energy and utilities, and SLED in the United States. For certain questions, participants could choose more than one response. In these cases, the responses do not round to exactly 100%. To download the core report, AT&T Cybersecurity Insights Report: Securing the Edge, click here.

EXECUTIVE SUMMARY

Edge means different things to different people, and vendors are defining edge according to their technology stacks. The ambiguity complicates security decisions. If this sounds familiar, it is. Consider what happened when cloud first emerged. Cloud was a momentous shift in IT and security, and so is edge, which moves computing from a centralized model to a decentralized model. The change is occurring in these motions:

- Away from datacenter consolidation
- Toward further distribution; on-premises and across cloud
- Toward placement of infrastructure, applications, and workloads, closer to where data is generated or consumed

Decentralization moves operations away from "lights on" monolithic applications to "thing enabled" computing experiences that are fully democratized. In the near future, expect to see small, high-quality, ephemeral, data-focused applets that live at the edge.

A proactive stance on security best serves enterprises that are innovating at the edge. The stakes are too high for reactionary security decisions or security controls prescribed based primarily on past experiences or practices. Sensors and data are everywhere, and networks are always available.

Edge networks are being implemented for specific use cases to help drive business. A useful approach for decision makers is to think about this transition through the lens of security, risk appetite, innovation goals, and network strategy — considerations that carry forward from previous AT&T Cybersecurity Insights reports. In *5G and the Journey to the Edge,* for example, 56% of survey respondents said they understood that 5G will require a change to their security approach to accommodate network changes. In the 2022 core report, *AT&T Cybersecurity Insights Report: Securing the Edge*, respondents weigh in on security controls and anticipated investments within their chosen edge network, the perceived associated risk, and benefit/cost considerations.

AT A GLANCE

KEY STATS

- 50% of manufacturing respondents state that they are in the mature stage of deploying edge initiatives.
- 52% of manufacturing edge network use cases are in the mature stage of deployment.
- Video-based quality inspection in manufacturing is one of two use cases, globally and across industries, with the highest rate of mature stage adoption (59%).

KEY TAKEAWAYS

There is not a one-size-fits-all security plan for the variety of use cases that are being deployed. Security teams need to be aware of all the security oversights and pitfalls that could impact the innovation enabled by edge computing in the manufacturing industry.

INTRODUCTION

This report is related to the broader 2022 *AT&T Cybersecurity Insights Report: Securing the Edge* and highlights specific manufacturing industry findings. The evolution of manufacturing and a greater need for digital technology is becoming increasingly apparent as manufacturers continue the path of convergence of information technology (IT) and operational technology (OT). Manufacturing organizations are moving forward with use cases such as smart warehousing, transportation optimization, intelligent inventory, augmented maintenance, and video-based quality inspection. 5G technology is transforming manufacturing at the edge in groundbreaking ways.

Edge computing allows for a wide variety of innovative use cases that at their core, consume, process, and create data. The location of this data, regardless of the length of time it resides there, will continue to increase the attack surface manufacturers need to protect. Today, cybersecurity practitioners in manufacturing seek to improve their abilities to ward off threats including attacks against users and endpoints, ransomware, and attacks against applications, servers, and data at the network edge. With edge, practitioners must now apply cybersecurity controls differently to safeguard the data and other digital assets that reside inside and outside manufacturing facilities. The mix of controls will include those used in the past as well as new and evolving technologies and platforms such as extended detection and response (XDR) and secure access service edge (SASE), which bring together a variety of security controls suited for distributed and cloud-based networks and edge use cases.

It is worth noting how valuable and potentially at risk the data is in manufacturing edge computing. Intellectual property, strategic marketing and business plans, sensor data, product cost information, operations data, and customer information can land in unauthorized hands with the potential to damage reputations and revenue. And, while data protection is critical, continuous operations of a manufacturing environment are paramount. If operations are interrupted, manufacturing organizations may face catastrophic consequences as a result. Keeping the manufacturing floor safe, optimized, and continuously operating are challenges faced by manufacturers.

78% of manufacturing respondents globally are planning, have partially implemented, or have fully implemented an edge use case.

THE STATE OF MANUFACTURING EDGE

ADOPTION RATES VARY

The survey data behind the 2022 *AT&T Cybersecurity Insights Report* reveals a variety of edge computing use cases that accelerate digital transformation.

For context, the study examines three stages of edge compute adoption in six industries and industry-specific use cases. Of all the possible adoption phases studied, the ones that are farther along are of the most interest. Planning and proof-of-concept stages are grouped together as mid-stage phases, and partially implemented and fully implemented are in the mature stage. Of all general use cases expected to be in production within three years, industrial IoT or OT functions top the list. Edge computing is a relatively new technology, so even fully implemented use cases are ripe for change as new standards and regulations come to fruition. Given this reality, "full implementation" may be transitory.

Industries studied in this survey – energy, finance, manufacturing, retail, U.S. public sector (SLED), and healthcare – are not uniform in their deployment stages. Retail, SLED, and manufacturing lead the mature stage, with 52%, 52%, and 50%, respectively. Manufacturing ranks highest in partial implementation, the top stage for all industries except energy and utilities. Globally and across industry use cases, video-based quality inspection, asset instrumentation and monitoring, and transportation optimization are among the top use cases in manufacturing with the highest rate of mature stage adoption. Augmented maintenance, inventory intelligence, and smart warehousing rank are the highest ranked manufacturing use cases in the mid-stage.

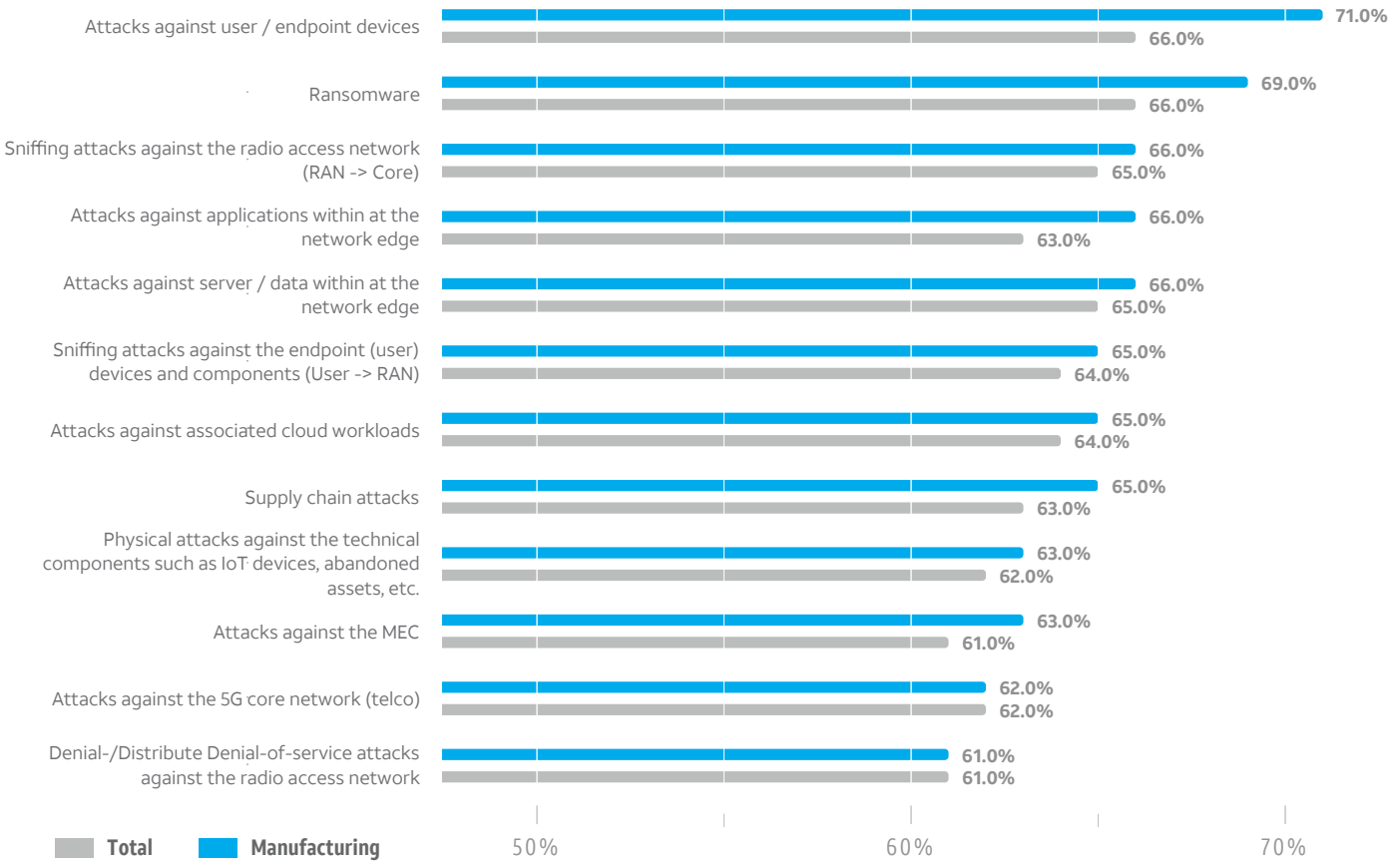
Video-based quality inspection, ranked by 59% of respondents as the most mature use case, has surged in implementation in part because it is low in perceived risk. Skilled human quality control (QC) operators find visible and audible defects during video playback, but human QC capacity doesn't scale well, especially given the variety of files and formats in modern workflows. Adaptive streaming video packages further

FIGURE 1

MANUFACTURING PRIORITIZES ATTACKS SLIGHTLY DIFFERENTLY THAN OTHER INDUSTRIES

Q. In your opinion, how likely are the following attack vectors? (Scale: 1 = very unlikely; 5 = very likely)

% of respondents that rated these categories as 4 or 5



N= 1520

BASE 1,520 (total); 258 (manufacturing)

SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

hamper scalability. Humans introduce subjectivity and the risk of introducing new defects because of manual activities and practices. To support scalability in multiple, geographically dispersed facilities, manufacturers are turning to edge computing and the use of artificial intelligence (AI) and IoT-driven automation. Edge computing can be paired with public or private 5G to support video-based quality inspection with increased bandwidth and low latency.

EDGE SECURITY x MANUFACTURING

In manufacturing, 78% of respondents globally are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE
The video-based quality inspection use case ranks highest within manufacturing for full or partial implementation. It is also one of the lowest in perceived risk.

EDGE ADVANTAGE
Edge computing offers reduced bandwidth, lower latency, and proximity of data, enabling companies to efficiently deploy specialized AI-inspection models across multiple, global facilities that can handle the large number of files and formats typically found in a modern workflow.

SECURITY CONTROLS
Manufacturing respondents rank intrusion and threat detection, device authentication, and data leakage monitoring among the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

71%

of respondents in manufacturing are most concerned about attacks against user and endpoint devices

THREAT VECTORS TO CONSIDER

Manufacturing security architects and leaders need to be aware of various types of attacks as use cases are planned, piloted, and rolled out. The coming together of IT and OT presents well-known challenges such as disparate team perspectives, insufficient communication between teams, and older devices not engineered for security. Further, it may be challenging to collect and normalize data for monitoring purposes, given the increase in data across merged IT/OT networks. Because of these challenges, the risk of attacks are higher.

Across all industries surveyed, ransomware is a top concern; however, it is the second-highest concern in manufacturing. Attacks against users and endpoints rank the highest. The three types of attacks that tied for third-highest concern in manufacturing are sniffing attacks against the radio access network (RAN), attacks against servers and data at the network edge, and attacks against applications at the network edge (see Figure 1). Manufacturers express these concerns because of the unique interdependencies of devices and the necessity of protecting those devices and associated software that facilitate materials movement and production. If an attack brings down a single device in a warehouse, an entire line can go down.

CYBERSECURITY CONTROL OPTIONS

No single control is a panacea to secure manufacturing assets, applications, and data. On the contrary, survey results show that manufacturing businesses use a combination of cybersecurity controls in their approach to securing business at the edge.

First, controls "on" the edge at the ingress-egress point can be grouped into general-purpose traditional controls (firewall, virtual private network [VPN], intrusion detection systems [IDS]) and special-purpose controls that can serve specific needs. Second, controls "in" the edge protect individual devices to fulfill a Zero Trust strategy and architecture. Controls that are put in place are dependent on the use case in question, and the networks that need to be secured are tied to the use case.

The types of devices that are utilized "in" edge computing can limit some of the security controls that potentially can be used. For example, not all of the device types in manufacturing can support security endpoint agents, so other compensating controls need to be put into place. In situations where sensitive data is not or cannot be encrypted completely, IDS is one example of a control that can be utilized to partially remediate the lack of complete encryption.

Figure 2 shows the mix of preferred manufacturing security controls, along with types of controls and where they will be deployed. The high ranking of on-premises security may be surprising to some when cloud computing garners so much attention. However, given the use cases and locations of manufacturing edge computing, on-premises security is a suitable and preferred choice.

The 2022 *AT&T Cybersecurity Insights Report: Securing the Edge* survey reveals the low current or planned use of patching as one of the layers of protection. Only 29% of manufacturing participants selected patching as a control they expect to deploy to protect the components of their primary use case. Likely reasons for the low ranking? Video cameras may not be supported with timely updates, and IT and security teams may have less visibility in environments where edge devices are used. Teams may lack resources to test patches and validate any negative impact on operations, or teams may lack a systematic way of deploying patches to devices using niche operating systems. And patching is a reactionary, manual, time-consuming control that isn't suited to the edge, where controls need to be automated and seamless. As a result, manufacturers rely on other controls to secure devices and applications.

Security architects need to recognize the challenges in keeping edge devices properly patched. Having a good foundation in manufacturing edge computing networks means incorporating compensating controls to proactively make up for known weaknesses in areas such as patching.

SECURITY INVESTMENTS

Cybersecurity leaders for the most part have made inroads in gaining increased budgets over the years. During the COVID-19 pandemic, IDC research has shown that cybersecurity budgets have generally increased. The general awareness of the need for security investments over the years, along with the need to secure data regardless of where it resides, has aided CISOs in seeing a significant percentage of edge computing budgetary dollars allocated to security (see Figure 3).

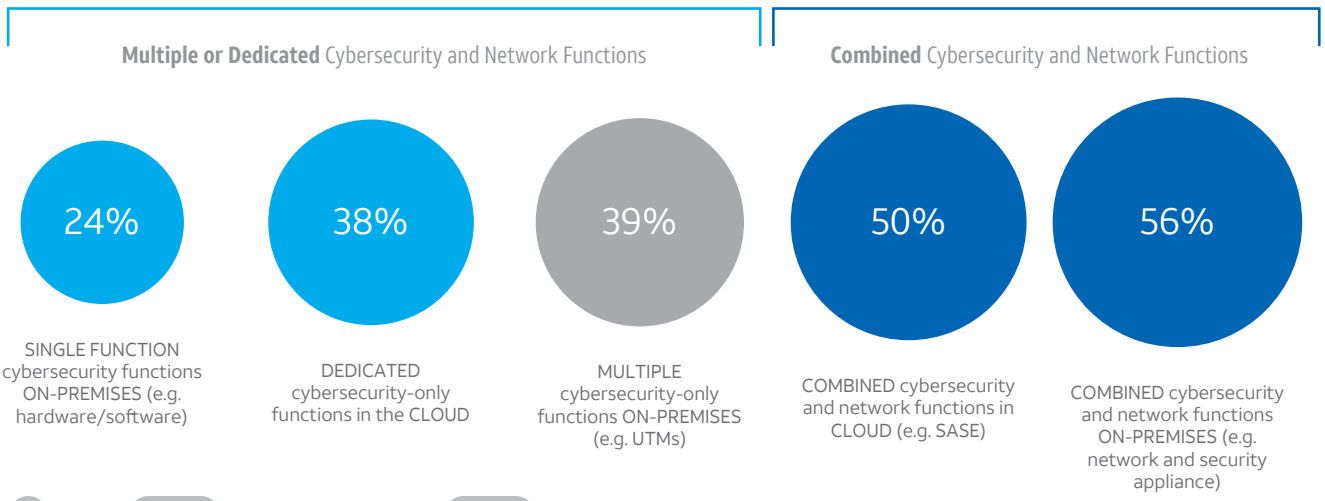
Given the array of sensitive data in manufacturing, the growth in IoT devices, and the challenges of merging IT and OT, it is encouraging to see that 50% of manufacturing respondents say they are investing between 11 – 20% of the total use case budget in security.

FIGURE 2

CYBERSECURITY CONTROLS WILL BE A MIX OF CLOUD AND ON-PREMISES FUNCTIONS

Q. How will you implement your CYBERSECURITY functions for your primary use case?

% of respondents



N= 1520 BASE 258 (manufacturing) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

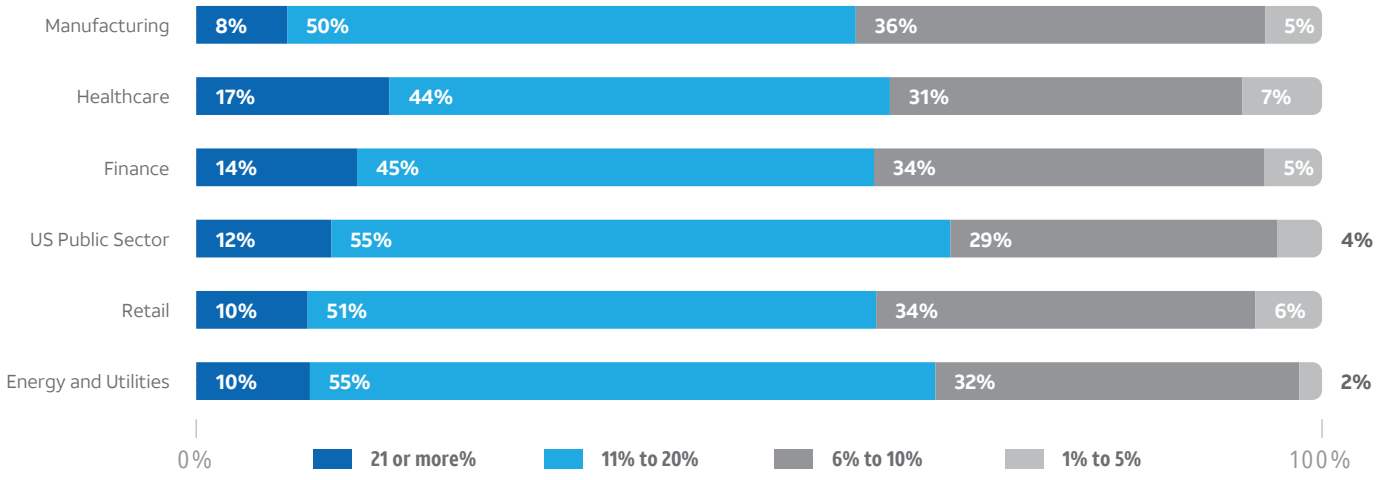
FIGURE 3

COMPANIES PLAN SIGNIFICANT INVESTMENTS TO SECURE EDGE USE CASES

Q. What percent of your organization's total COMBINED investment for ALL of these use cases (in production within 3 years) do you anticipate being allocated directly to security?

% of respondents

Combined Investment Allocated to Security by Industry



N= 1520 BASE 1,520 (total); 258 (manufacturing) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

Note: This data does not include 'don't know' survey responses.

CYBERSECURITY CONTROLS: TOTAL COST OF OWNERSHIP AND EFFECTIVENESS

Total cost of ownership (TCO) and effectiveness are core considerations for security decision makers as they evaluate the mix of cybersecurity controls. Of all controls studied and across all industries, passwords have the lowest TCO and intrusion detection solutions (IDSs) have the highest TCO.

Compared to other industries, manufacturing respondents have the third-highest TCO on their cybersecurity controls. Based on survey responses, manufacturing respondents rank intrusion and threat detection, device authentication, and data leakage monitoring among the most efficient and effective security controls available. Device authentication offers a low TCO and allows the use of certificates to secure devices prior to shipment and by enterprises to secure the devices on their networks. This is essential for understanding attack and protection surface mapping.

Consider how these findings of TCO of security controls apply to the top use case of video-based quality inspection. Personnel involved with video-based quality inspection are likely using physical computers to log in to do their jobs.

Network access control (e.g., ZTNA) and distributed denial of service (DDoS) are perceived to be less effective and have a lower TCO Given the still-early efforts to bring together IT and OT, network access control is likely nascent and in limited use. And, while DDoS is not a top choice in manufacturing, it may be seen as a necessary preventive measure.

Regarding the effectiveness of controls, IDS received the highest effectiveness ranking from all industries, followed closely by data encryption at rest and internally encrypted traffic. Compared with all other industries, manufacturing believes that device authentication is highly effective; however, the top manufacturing control ranked for effectiveness is network access restrictions followed by patching. IDS receives the lowest effectiveness in manufacturing. The high and low rankings appear to align with current manufacturing realities associated with the challenges of merging IT and OT while innovating at the edge.

RECOMMENDATIONS

- Use the movement to the edge to unify traditional IT and OT teams. While these teams may have two unique perspectives on security, each team can benefit from a collaborative and congenial partnership. Remember, security is a combination of people, process, and technology. Take advantage of different perspectives to bolster overall security for your manufacturing organization.
- Know your data! The edge is all about data – moving applications, workloads, and hosting closer to where data is being created and consumed. Take the opportunity to add data scientists to your team to analyze the overwhelming amount of data collected at the edge. In turn, data scientists can work with the SOC team to potentially and proactively identify threats.
- Satisfy the needs of customers and partners with a transparent supply chain. By delivering more transparency, security controls show points of strength as well as potential points of weakness in a supply chain. This transparency helps to identify vulnerabilities.
- Delve into the shared security responsibility model with public cloud service providers and carriers to clarify roles and responsibilities at every stage of use case implementation.
- Ask for help. Engage security services providers with broad, complementary capabilities to help reduce complexity, lower cost, enable rapid scalability, and increase organizational agility.

CONCLUSION

Manufacturing is in the midst of tremendous transformation that will have far-reaching impacts, and many companies are proactively looking for support in securing IT and OT environments more holistically . From securing supply chains of the most critical of products to streamlining the manufacturing environment for near real-time defect remediation, change is happening and security is a central tenet. The convergence of IT and OT is real, providing value through process improvements and network modernization that looks to implement the tenets of Zero Trust – especially in the areas of network segmentation, access management and control, and DDoS protection. Manufacturing organizations see the benefits of adopting edge use cases to ease constraints across locations, platforms, and partners. The strong understanding, adoption, and movement to edge computing will help the business of manufacturing, and new edge use case practices have the potential to deliver better quality products and experiences. Those manufacturing organizations that are quick to realize that security is not a technical problem to be solved, but rather a business enabler may be capable of delivering stronger and more predictable outcomes.

ABOUT AT&T CYBERSECURITY

AT&T Cybersecurity helps make your network more resilient. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and security operations center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

CONTRIBUTING ORGANIZATIONS

AT&T Business

MANUFACTURERS ARE INNOVATING AT THE EDGE. SECURITY TEAMS SHOULD WORK COLLABORATIVELY TO AVOID ANY PITFALLS AND CONTINUE ON A PATH TO TRANSFORMATION.