livingsecurity

PacLife CISO Report:

Intelligent Metrics & Insurance Threat Landscape

EXECUTIVE SUMMARY:

- Pacific Life's attack surface includes legacy software, third party vendors (e.g. AWS, Salesforce), and a large enterprise footprint of employees, contractors and consumers
- Despite investments/advancements made into security technologies, human error remains the top security risk to Pacific Life[1]
- PacLife's sample engagement with the Living Security Platform showed that while participation was higher than average, awareness of certain key topics (e.g. data classification, data destruction, PII) left room for improvement
- The Living Security Platform provides training modules that address these specific deficiencies as well as next-gen reporting (NGR) that will provide visibility into human risk as a security score, trendline and progress across time

INSURANCE INDUSTRY THREAT LANDSCAPE:

PacLife's emphasis on transforming IT from a dependence on legacy software to cloud technologies brings both opportunities and threats from a security standpoint,[2] and introduces a different kind of human element that must be secured. Examples include training users on cloud privacy settings, configuration, credential management and insider threat (among other things).[3] Cloud services provide some of the best tools to ensure data is protected from malicious actors, but human error can render these tools useless if and when misconfiguration occurs or credential mismanagement happens. It is vital that employees are provided with awareness materials surrounding cloud security threats (etc.) to avoid becoming accidental insider threats or facilitating data breach.

As a leading insurer in B2B and B2C, PacLife also has to account for a large enterprise footprint of devices, suppliers and partners to support life insurance, mutual fund and annuity product lines.[4] Data breach is the biggest threat looming over this large attack surface. Not only do employees have to be trained on the importance of protecting personally identifiable information (PII), but the supporting cast of vendors, co-processors and consumers must also possess some level of security awareness.

To address these problem areas, PacLife may consider using the Living Security Platform to disseminate training modules on cloud security threats, data classification, authentication and synthetic identity theft (etc.) to increase situational awareness of new and emerging threats online and maintain compliance with Federal regulations (e.g PCI).

PacLife's sample (n=17) engagement with the Living Security Platform reflects this conclusion, with some of the lowest scores (areas of weakness) including data classification (23% correct), data destruction (50%) and the definition of PII (75%) On the upside, the proportion of overall engagement (76%) from PacLife users on the Platform (for True Eye series) was higher than average.[5]

Moving forward, Living Security's Platform Content and Next-Gen Reporting (NGR) will allow PacLife administrators even more visibility into these human risk metrics by offering advanced security scores by category, trending across time, the identification of high-risk participants and participant progress over time.

---

[1] https://livingsecurity.com/blog/dbir-security/ - The 2020 Verizon DBIR supports this claim as the only action type that consistently increases year-over-year is error

[2] https://aws.amazon.com/solutions/case-studies/pacific-life-insurance/

[3] https://ls.livingsecurity.com/cloudsecuritythreat

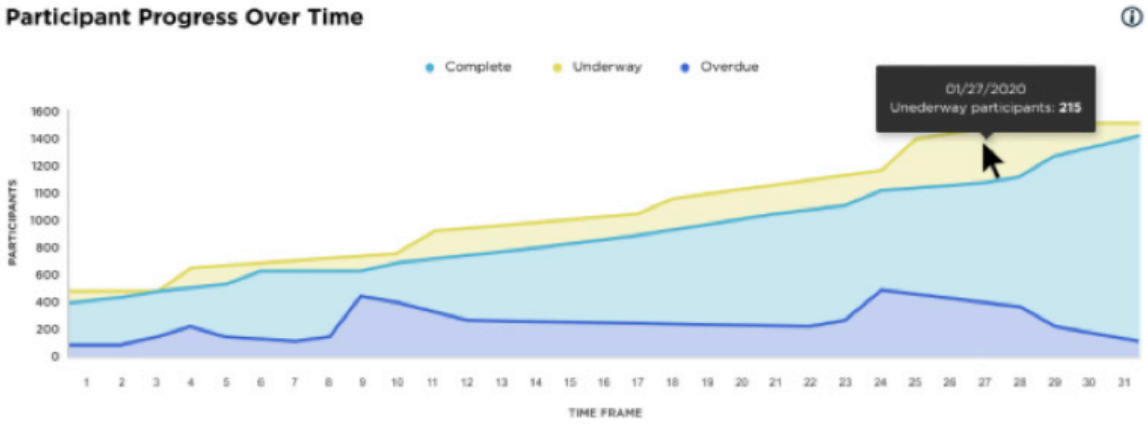
[4] https://www.pacificlife.com/

[5] Overall generalizability of data is low, because the overall sample size is so small.

EXAMPLES NEXT-GEN REPORTING & INTELLIGENT METRICS

THE OVERALL SECURITY SCORE is a weighted average of performance among each of the 10 security categories and influenced by user engagement and tenure on platform.

A HIGH-RISK PARTICIPANT is considered someone who is a new user (unproven track record), a low-engager (below a certain threshold of interactivity) or a poor-performer (below a certain threshold of acceptable performance).



PARTICIPANT PROGRESS OVER TIME simply measures participants' progress through training as it evolves day-to-day. As users engage with or complete modules and assigned training, the trend-lines associated with progress will rise.