DELL Technologies

5 안전한 혁신 환경을 위한 권고

1	2	3	4	5
일찍, 자주 소통	**보안 스택의 합리화 및 간소화**	**사이버 보안 가드레일 정립**	**유연성 유지, 창의성 확보**	**강력한 보안 문화 조성**
경영진 및 주요 이해 관계자 참여 유도	복잡성 감소	정책 정의	새로운 보안 방법을 개방적으로 수용	광범위한 참여 촉진
혁신 계획 숙지	중복 제거	액세스 제어 구현	혁신을 수용하는 보안 방법에 집중	투명성 제고
보안 팀이 대화를 시작할 수 있도록 지원	단일 창구 생성	논리적 및 물리적 시스템 간 통합	보안 담당 부서에서 혁신을 촉발할 수 있음을 유념	협업 주도
	탄탄한 구매 평가 프로세스 개발			

안전한 혁신 환경 조성

기술 및 데이터 중심 세계에서 혁신을 극대화하려면 혁신을 지원하도록 사이버 보안을 구축해야 합니다. 그러면 기업과 조직은 어떻게 보안을 유지하면서 성장, 창의성 및 혁신을 지원하는 환경을 조성할 수 있을까요?

이러한 환경의 실제 사례를 조사하기 위해 Dell Cybersecurity Marketing 팀의 Sameer Shah 씨가 애리조나 길버트 타운의 CISO(Chief Information Security Officer)인 Tony Bryson 박사를 만나 혁신적인 미래 도시 이니셔티브와 이를 추진하는 데 보안이 어떤 역할을 하는지에 대해 논의했습니다.

Bryson 박사의 권고를 요약한 내용을 읽어 보시기 바랍니다. 전체 대화를 보려면 **dell.com/cybersecuritymonth**를 방문하십시오.

> [이해 관계자들이] 무엇을 원하는지 그리고 비즈니스와 고객에게 유리한 기술과 혁신을 얼마나 활용할 의향이 있는지 확인하십시오."
>
> **Tony Bryson** 박사, 길버트 타운
> CISO(Chief Information Security Officer)

미래 도시

길버트 타운의 미래 도시 이니셔티브는 데이터를 사용하여 시민들의 삶을 풍요롭게 만드는 지속 가능하고 회복탄력적인 인프라스트럭처를 구축하도록 설계되었습니다. 기술은 청구서 지불부터 교통 관리, 급수, 수질에 이르기까지 서비스 제공에 크게 관여합니다. 또한 데이터를 수집하여 향후 서비스 사용량과 요구량을 예측하는 데에도 관여합니다. 이 이니셔티브는 끝이 있는 유한한 것이 아니라 끊임없이 발전하는 반복적인 프로세스입니다.

첫 번째 CISO로서 Bryson 박사의 임무는 사이버 보안에 대해 더욱 전략적인 접근 방식을 취하는 것이었습니다. 현대적인 기술 기반 도시 서비스를 제공하려면 도시의 야심 찬 목표를 지원하기 위해 고안된 강력한 데이터 보호, 분류 및 제어 기능이 필요합니다.

이 프로세스를 계속 성공적으로 진행하면서 Bryson 박사는 성공을 촉진하고 안전하게 성장하면서 혁신할 수 있는 올바른 환경을 조성하기 위한 몇 가지 주요 권고 사항을 파악하게 되었습니다.

일찍, 자주 소통

Bryson 박사는 혁신 프로세스 초기에 경영진과 기타 주요 이해 관계자를 참여시켜야 한다고 강조했습니다. 그는 "그들이 무엇을 원하는지 그리고 비즈니스와 고객에게 유리한 기술과 혁신을 얼마나 활용할 의향이 있는지 확인하십시오."라고 말했습니다.

조기 커뮤니케이션을 자연스럽게 확장하려면 혁신 주기 초반에 사이버 보안 관련 대화를 나누는 것이 필요하며, 사이버 보안 팀은 핵심 파트너로서 이러한 논의의 촉매가 될 수 있습니다.

길버트 타운의 AI 사용이 대표적인 사례입니다. 보안 담당 부서에서는 2년 전에 이러한 대화를 시작했으며 AI 생성 데이터를 어떻게 신뢰할 것인지, 어떻게 저장할 것인지, 어떤 방식으로 주민들이 AI 사용을 적절히 이해하도록 할 것인지 등에 대한 중요한 질문을 던지는 데 주도적인 역할을 했습니다. 이로 인해 다부서 위원회가 설립되고, 미국 서부에서 최초로 정규직 CAIO(Chief Artificial Intelligence Officer)를 고용하게 되었습니다.

"이러한 혁신을 방해하는 기존의 보안 방식에 안주했다면 절대 이러한 성과를 거둘 수 없었을 것입니다."라고 Bryson 박사는 말합니다. "혁신을 시도하고 올바른 방식으로 일을 하려면 대화가 먼저입니다."

보안 스택의 합리화 및 간소화

Bryson 박사가 우선적으로 한 일은 각 제품 및 서비스의 용도를 파악하기 위해 보안 스택의 인벤토리를 작성하는 것이었습니다. 이러한 노력 덕분에 중복된 부분을 상당히 많이 찾아냈습니다. 축소와 합리화는 비용을 절감하지만, 그보다 더 중요한 점은 소규모 보안 팀이 단일 창구와 단일 정보 소스를 통해 사이버 보안 기능을 관리하고 문제를 해결할 수 있다는 것입니다.

Bryson 박사는 사이버 보안의 적은 복잡성이라는 오래된 격언을 들려주면서 "저는 사람들이 무슨 일이 벌어지고 있는지를 파악하기 위해 여러 시스템 사이를 오가는 것을 원치 않습니다."라고 말했습니다.

올바른 사이버 보안 가드레일 정립

조직 내 혁신가들은 시스템과 데이터를 안전하게 보호하는 보안 지침을 숙지하고 준수해야 합니다. 이러한 규칙은 정책이나 액세스 제어일 수도 있고, 혁신가가 경쟁의 장을 이해하는 데 도움이 되는 기타 원칙이 될 수 있습니다. 이 경쟁의 장은 보안과 혁신가 사이의 효과적인 파트너십을 통해 만들어지는 혁신을 위한 안전한 환경입니다.

유연성 유지, 창의성 확보

Bryson 박사는 사이버 보안 표준을 정립하고 시행하는 것이 중요하지만 혁신에는 때때로 유동성과 창의성이 필요하다고 언급했습니다. 그는 이렇게 말했습니다. "혁신은 사업부에서만 일어나는 것이 아닙니다. 혁신이 정보 기술 내에서 그리고 정보 보안 담당 부서에서 일어나는 경우도 많습니다. 기업 혁신에 맞춰 시스템과 데이터를 보호하는 새롭고 창의적인 방법을 찾아야 할 수도 있습니다. 그러니 이에 대비하십시오."

DELL Technologies

탄탄한 사이버 보안 문화 조성

Bryson 박사는 탄탄한 보안 문화를 발전시키는 것이 중요하다고 강조했습니다. "사이버 보안에 관해서는...문화가 가장 중요합니다. 사람들이 사이버 보안을 의식하는 문화가 없다면 위협 노출 범위를 더 커질 수밖에 없습니다."

탄탄한 사이버 보안 문화를 조성하기 위해서는 개방적이고 투명한 대화, 폭넓은 참여, 명확하게 정립된 표준, 내부 및 외부 보안 팀과 고객 간의 협력 정신 등 이미 논의된 많은 요소가 토대가 되어야 합니다.

성장이 가속됨에 따라 사이버 보안은 방어에 중점을 둔 사후 대응적 자세에서 긍정적인 결과를 촉진하는 사전 예방적 접근 방식으로 발전해야 합니다.

기업과 조직은 혁신을 보호할 뿐만 아니라 강화할 수 있는 현대적인 보안 사고 방식을 도입해야 합니다.

이는 보안 조치를 개발 프로세스에 통합하는 커뮤니케이션과 협업을 통해 달성할 수 있습니다. 목표는 보안을 유지하면서 창의성이 꽃을 피울 수 있게 만드는 환경입니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

DELL Technologies